(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月11 日 (11.08.2005)

PCT

(10) 国際公開番号
WO 2005/073843 A1

(51) 国際特許分類[7]: G06F 9/06, 9/445, H04M 1/00

(21) 国際出願番号: PCT/JP2005/001232

(22) 国際出願日: 2005 年1 月28 日 (28.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-019461 2004 年1 月28 日 (28.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 川口 京子 (KAWAGUCHI, Kyoko).

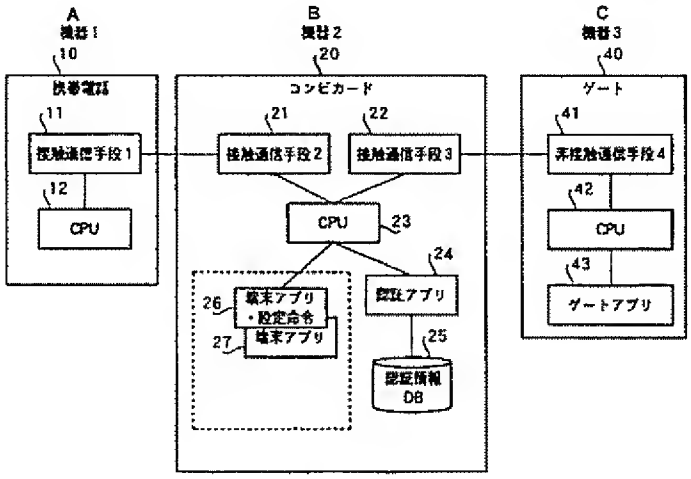
(74) 代理人: 鷲田 公一 (WASHIDA, Kimihito); 〒2060034 東京都多摩市鶴牧１丁目２４−１新都市センタービル５階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: SECURE DEVICE, TERMINAL DEVICE, GATE DEVICE, AND DEVICE

(54) 発明の名称: セキュアデバイス、端末装置、ゲート機器、機器



A DEVICE 1
B DEVICE 2
C DEVICE 3
10 MOBILE TELEPHONE
11 CONTACT COMMUNICATION MEANS 1
20 COMBINED CARD
21 CONTACT COMMUNICATION MEANS 2
22 CONTACT COMMUNICATION MEANS 3
26 TERMINAL APPLICATION/SETTING INSTRUCTION
27 TERMINAL APPLICATION
24 AUTHENTICATION APPLICATION
25 AUTHENTICATION INFORMATION DB
40 GATE
41 NON-CONTACT COMMUNICATION MEANS 4
43 GATE APPLICATION

(57) Abstract: There are provided a secure device, terminal device, a gate device, and a device providing a secure device such as an IC card capable of limiting an area where the card application function and the device function are realized. The secure device (20) includes: an authentication application (24) for performing authentication of a gate device (40); a terminal application/setting instruction (26) and a terminal application (27) installed in a mobile telephone (10) as a terminal; and a CPU (23) as control means for installing the terminal application specified by the gate device (40) in the mobile telephone (10) when authentication application (24) has successfully authenticated the gate device (40). The secure device (20) is held over the gate device (40) and only in the area where normally passed, the terminal application/setting instruction (26) and the terminal application (27) are installed in the mobile telephone (10). Since the gate application (43) of the gate device (40) specifies an application which functions in a particular area, a user need not perform registration operation. Moreover, there is no need of mounting a GPS receiver or the like onto the terminal.

[続葉有]

WO 2005/073843 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: カードアプリ機能や装置機能等が発現されるエリアを限定できるＩＣカード等のセキュアデバイスを提供するセキュアデバイス、端末装置、ゲート機器、機器。セキュアデバイス（２０）に、ゲート機器（４０）に対して認証処理を行う認証アプリ（２４）と、端末である携帯電話（１０）にインストールする端末アプリ・設定命令（２６）や、端末アプリ（２７）と、認証アプリ（２４）がゲート機器（４０）との認証に成功した場合に、ゲート機器（４０）から指定された端末アプリを携帯電話（１０）にインストールする制御手段であるＣＰＵ（２３）とを設けている。セキュアデバイス（２０）をゲート機器（４０）に翳し、正常に通過したエリアでのみ、端末アプリ・設定命令（２６）、端末アプリ（２７）が携帯電話（１０）にインストールされる。ゲート機器（４０）のゲートアプリ（４３）が特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末へのＧＰＳ受信機等の装備も必要がない。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001232

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F9/06, G06F9/445, H04M1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F9/06, G06F9/445, H04M1/00, G06F15/00, G06F17/60, G06K17/00, G06K19/00, G06F12/14, G07C9/00, E05B49/00, G08B25/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JST FILE(JOIS), CSDB(Japanese Patent Office)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2003-281587 A (Seiko Epson Corp.), 03 October, 2003 (03.10.03), Full text (Family: none)	8,17,18 9
A	JP 6-187163 A (Sony Corp.), 08 July, 1994 (08.07.94), Full text (Family: none)	1-7,10-16
A	JP 6-119265 A (Matsushita Electric Industrial Co., Ltd.), 28 April, 1994 (28.04.94), Full text & CA 2106122 A	1-7,10-16

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 February, 2005 (21.02.05)	08 March, 2005 (08.03.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001232

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 7-200756 A (Toppan Printing Co., Ltd.), 04 August, 1995 (04.08.95), Par. Nos. [0004], [0005], [0007] (Family: none)	4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001232

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

(See extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

Claims 1-7, 10-16 constitute a first group while claims 8, 9, 17, 18 constitute a second group. The first group includes the configuration that a gate device specifies the application to be installed. However, this configuration is not included in the second group. Accordingly, the matter common to the first group and the second group is only the configuration that authentication is performed between the gate device and the secure device.

However, the search has revealed that the aforementioned "common matter" is not novel since it is disclosed in

document: JP 2003-281587 A (Seiko Epson Corp.), 03 October, 2003 (03.10.03), full text (family none).

As a result, the aforementioned "common matter" makes no contribution over the prior art and this "common matter" cannot be a special technical feature within the meaning of PCT Rule 13.2, second sentence.

Accordingly, there exists no "special technical feature" common to all the inventions of claims 1-18.

Since there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence, no technical relationship within the meaning of PCT Rule 13 between the different inventions can be seen.

Consequently, it is obvious that the inventions of claims 1-18 do not satisfy the requirement of unity of invention.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

WASHIDA, Kimihito
5th Floor, Shintoshicenter Bldg., 24-1, Tsurumaki
1-chome, Tama-shi Tokyo
2060034
JAPON

26. 2005

Date of mailing *(day/month/year)* 13 April 2005 (13.04.2005)	
Applicant's or agent's file reference 2F04264-PCT	**IMPORTANT NOTIFICATION**
International application No. PCT/JP05/001232	International filing date *(day/month/year)* 28 January 2005 (28.01.2005)
International publication date *(day/month/year)*	Priority date *(day/month/year)* 28 January 2004 (28.01.2004)
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al	

1. By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. *(If applicable)* The letters "NR" appearing in the right-hand column denote a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

3. *(If applicable)* An asterisk (*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b) (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
28 January 2004 (28.01.2004)	2004-019461	JP	24 March 2005 (24.03.2005)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 740 14 35

Authorized officer
Hammouda Abdessalem

Facsimile No. +41 22 338 90 90
Telephone No. +41 22 338 7119

特許協力条約に基づく国際出願願書

紙面による写し（注意：電子データが原本となります）

0	受理官庁記入欄	
0-1	国際出願番号	
0-2	国際出願日	
0-3	(受付印)	

0-4	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、	
0-4-1	右記によって作成された。	JPO-PAS 0322
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	2F04264-PCT
I	発明の名称	セキュアデバイス、端末装置、ゲート機器、機器
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除く全ての指定国 (all designated States except US)
II-4ja	名称	松下電器産業株式会社
II-4en	Name:	MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.
II-5ja	あて名	5718501 日本国 大阪府門真市大字門真１００６番地
II-5en	Address:	1006, Oaza Kadoma, Kadoma-shi Osaka 5718501 Japan
II-6	国籍(国名)	日本国 JP
II-7	住所(国名)	日本国 JP
II-8	電話番号	06-6908-1473
II-9	ファクシミリ番号	06-6909-0053
II-11	出願人登録番号	000005821
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	川口　京子
III-1-4en	Name (LAST, First):	KAWAGUCHI, Kyoko
III-1-5ja	あて名	
III-1-5en	Address:	
III-1-6	国籍(国名)	
III-1-7	住所(国名)	

特許協力条約に基づく国際出願願書

紙面による写し（注意：電子データが原本となります）

IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)	
IV-1-1ja	氏名(姓名)	鷲田　公一	
IV-1-1en	Name (LAST, First):	WASHIDA, Kimihito	
IV-1-2ja	あて名	2060034 日本国 東京都多摩市鶴牧１丁目２４－１新都市センタービル５階	
IV-1-2en	Address:	5th Floor, Shintoshicenter Bldg., 24-1, Tsurumaki 1-chome, Tama-shi Tokyo 2060034 Japan	
IV-1-3	電話番号	042-338-4600	
IV-1-4	ファクシミリ番号	042-338-4605	
IV-1-6	代理人登録番号	100105050	
V	国の指定		
V-1	この願書を用いてされた国際出願は、規則4.9(a)に基づき、国際出願の時点で拘束される全てのPCT締約国を指定し、取得しうるあらゆる種類の保護を求め、及び該当する場合には広域と国内特許の両方を求める国際出願となる。		
VI-1	先の国内出願に基づく優先権主張		
VI-1-1	出願日	2004年 01月 28日 (28.01.2004)	
VI-1-2	出願番号	2004-019461	
VI-1-3	国名	日本国 JP	
VI-2	優先権証明書送付の請求 上記の先の出願のうち、右記の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁に対して請求している。	VI-1	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	申立て	申立て数	
VIII-1	発明者の特定に関する申立て	-	
VIII-2	出願し及び特許を与えられる国際出願日における出願人の資格に関する申立て	-	
VIII-3	先の出願の優先権を主張する国際出願日における出願人の資格に関する申立て	-	
VIII-4	発明者である旨の申立て(米国を指定国とする場合)	-	
VIII-5	不利にならない開示又は新規性喪失の例外に関する申立て	-	
IX	照合欄	用紙の枚数	添付された電子データ
IX-1	願書(申立てを含む)	3	✓
IX-2	明細書	37	✓
IX-3	請求の範囲	3	✓
IX-4	要約	1	✓
IX-5	図面	38	✓
IX-7	合計	82	

特許協力条約に基づく国際出願願書

紙面による写し（注意：電子データが原本となります）

	添付書類	添付	添付された電子データ
IX-8	手数料計算用紙	－	✓
IX-11	包括委任状の写し	－	✓
IX-17	PCT-SAFE 電子出願	－	－
IX-19	要約書とともに提示する図の番号	1	
IX-20	国際出願の使用言語名	日本語	
X-1	出願人、代理人又は代表者の記名押印	/100105050/	
X-1-1	氏名(姓名)	鷲田　公一	
X-1-2	署名者の氏名		
X-1-3	権限		

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

明 細 書

セキュアデバイス、端末装置、ゲート機器、機器

技術分野

[0001] 本発明は、ICカード等のセキュアデバイスと、このセキュアデバイスとの間で接触通信または非接触通信を行う端末装置、ゲート機器、機器に関するものである。

背景技術

[0002] 近年、ICカードは、電子決済用カードや定期乗車券、イベント用チケット、クレジットカード等として広く利用されている。最近では、微細化技術の向上とも相俟って、比較的大容量の記憶空間を持つICカードが作られており、このようなICカードは、カードサービスを実行する複数のカードアプリケーション(以下、アプリケーションを「アプリ」と略称する)を格納することにより、一枚で複数の用途に対応するマルチアプリカードとして使用することができる。

[0003] ICカードの通信方式には、ICカードの電気的接点にリーダ・ライタを接触して記録情報の読み書きを行う接触通信と、無線通信で情報をやり取りし、リーダ・ライタとの物理的な接触を必要としない非接触通信との二通りがある。最近は、接触通信及び非接触通信の両方が可能なICカード(コンビカード)を携帯端末装置に搭載し、この携帯端末を電子財布や定期券の替わりに使用することも行われている。

[0004] 下記特許文献1には、搭載したマルチアプリカードから、目的のカード機能を迅速かつ簡単に選択することを可能にした携帯端末装置が開示されている。この装置を使用するユーザは、マルチアプリカードのカード機能を携帯端末の表示画面に一覧表示して、その中から親アプリと、親アプリに関連付けたアプリ(優先アプリ)とを登録し、マルチアプリカードに記憶させる。例えば、親アプリとして定期乗車券機能を登録し、その優先アプリとして電子マネー機能を登録すると、携帯端末を自動改札装置に翳し、マルチアプリカードの定期乗車券機能を用いて駅構内に入場した場合に、携帯端末の表示画面には、優先アプリの電子マネー機能の表示順位を最上位に設定したアプリ選択画面が表示される。

[0005] また、ユーザがマルチアプリカードのアプリ機能を使用すると、その位置が携帯端

末のGPS受信機等の現在位置検出手段で検出されて、使用したアプリ機能と使用位置との関係が携帯端末で記憶される。そして、その位置付近を再び訪れたとき、携帯端末の表示画面には、その位置に対応するアプリ機能の表示順位を最上位に設定したアプリ選択画面が表示される。

特許文献1:特開2003－76958号公報

発明の開示

発明が解決しようとする課題

[0006] このように、場所と対応付けてアプリ選択画面の表示を変更することは前記特許文献1に記載されているが、ICカードのカード機能を場所によって限定する発想は、この文献には示されていない。ICカードのカード機能を場所で限定することができるならば、例えば、ICカードを搭載した携帯電話を、社内エリアでは内線電話として使用できるようにし、あるいは、ICカードに格納された特定データを社内エリアでのみ利用できるようにする等、新たな応用が可能になる。

[0007] また、ICカードのカード機能を場所によって限定する場合に、前記特許文献1のように、ユーザの登録操作を必要とするのでは、ユーザの処理負担が大きいし、また、携帯端末が位置情報の取得手段を持つ必要があるのでは、携帯端末のコストが高くなる。

[0008] 本発明の目的は、こうした従来の課題を解決するものであり、ユーザの処理負担やコスト負担を招かずに、セキュアデバイスのカード機能や、端末装置あるいは機器の機能を、場所と関連付けて変更したり、または通信方式、前回の無効化処理、さらにはメモリ容量等に応じて変更したり、よりセキュリティを確保することができるICカード等のセキュアデバイスを提供し、また、このセキュアデバイスと連携して処理を行う端末装置、ゲート機器、機器を提供することである。

課題を解決するための手段

[0009] 本発明のセキュアデバイスは、ゲート機器に対して認証処理を行う認証手段と、端末にインストールする端末アプリケーションと、前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定された端末アプリケーションを端末にインストールする制御手段と、を備える構成を採る。

[0010] また、本発明のセキュアデバイスは、ゲート機器に対して認証処理を行う認証手段と、カードアプリケーションと、前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定されたカードアプリケーションが、端末の端末アプリケーションのアクセスを許容する制御手段と、を備える構成を採る。

[0011] また、本発明のセキュアデバイスは、ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する認証手段と、前記認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対して、前記機器の検証に供するためにゲート機器の前記識別情報を送信し、または、前記機器に代わって前記識別情報を検証するカードアプリケーションと、を備える構成を採る。

[0012] また、本発明のゲート機器は、セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリケーションを指定するゲートアプリケーションと、を備える構成を採る。

[0013] また、本発明のゲート機器は、セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末の端末アプリケーションがアクセスできるカードアプリケーションを指定するゲートアプリケーションと、を備える構成を採る。

[0014] また、本発明の端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスから、前記ゲート機器が指定した端末アプリケーションをインストールする構成を採る。

[0015] また、本発明の端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスが保持するカードアプリケーションの中で、前記ゲート機器が指定したカードアプリケーションにアクセスする端末アプリケーションを備える構成を採る。

[0016] また、本発明の機器は、ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報を取得し、前記識別情報の検証に成功した場合に所定の動作を行う構成を採る。

[0017] また、本発明の機器は、ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行う構成を採る。

発明の効果

[0018] 本発明のセキュアデバイス、ゲート機器、端末装置及び機器は、連携して、セキュアデバイスのカード機能や、端末装置あるいは機器の機能を、場所と関連付けて変更したり、または通信方式、前回の無効化処理、さらにはメモリ容量等に応じて変更したり、よりセキュリティを確保することができる。例えば、端末装置の機能をオフィスの中と外とで切替えたり、特定の処理機能を限定したエリアでのみ可能にしたり、特定の入口から入場しなければ、部屋の扉や金庫が開かないようにしたりすることができる。また、こうした処理を、ユーザの処理負担やコスト負担を招かずに実現することができる。

図面の簡単な説明

[0019] [図1]本発明の第1の実施形態における携帯電話、コンビカード及びゲートの構成を示すブロック図

[図2]本発明の第1の実施形態に設定されたデータDBのデータ構成を示す図

[図3]本発明の第1の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図4]本発明の第1の実施形態における携帯電話、ICカード及びゲートの構成を示すブロック図

[図5]本発明の第2の実施形態における携帯電話、コンビカード及びゲートの構成を示すブロック図

[図6]本発明の第2の実施形態に設定されたデータDBのデータ構成を示す図

[図7]本発明の第2の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図8]本発明の第2の実施形態における優先度設定DBのデータ構成を示す図

[図9A]本発明の第2の実施形態における優先度設定DBの他のデータ構成であって、各カードアプリIDの優先度を規定した優先度テンプレートの一例を示す図

[図9B]本発明の第2の実施形態における優先度設定DBの他のデータ構成であって、ゲートアプリIDに対応して優先度テンプレートを設定した優先設定DBの一例を示す図

[図10]本発明の第3の実施形態におけるドア、ICカード及びゲートの構成を示すブロック図

[図11]本発明の第3の実施形態におけるドア、ICカード及びゲートの動作を示すシーケンス図

[図12]本発明の第3の実施形態におけるPIN入力部を持つドア、ICカード及びゲートの構成を示すブロック図

[図13]本発明の第3の実施形態におけるPIN入力部を持つドア、ICカード及びゲートの動作を示すシーケンス図

[図14]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の構成を示すブロック図

[図15]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図16]本発明の第4の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図17]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図(図16の続き)

[図18]本発明の第4の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図19]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図(図18の続き)

[図20]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図21]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図22]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の

動作を示すシーケンス図

[図23]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図24]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図25]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図26]本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス図

[図27]第5の実施形態における会社の入場処理と退場処理とを例にした認証情報DB例を示す図

[図28]第5の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図29]第6の実施形態の認証情報DBの内容の一例を示す図

[図30]第6の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図31]第7の実施形態の構成を示すブロック図

[図32]第7の実施形態の認証情報DBに設定されたデータの一例を示す図

[図33]第7の実施形態の端末設定管理部に設定されたデータの一例を示す図

[図34]第7の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図35]第8の実施形態の構成を示すブロック図。

[図36]第8の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図

[図37]第8の実施形態の端末アプリ退避管理部における詳細処理を示すフローチャート

発明を実施するための最良の形態

[0020] （第1の実施形態）

本発明の第1の実施形態では、セキュアデバイスであるICカードが特定エリアに位置するときだけ、ICカードに格納された端末アプリが、端末にインストールされる場合について説明する。

[0021] この特定エリアの入口にはゲートが在り、ゲートアプリは、ICカードとの認証処理に成功すると、ICカードに対して、端末に設定すべき端末アプリを指定する。これを受けて、ICカードは、適宜の時期に、保持する端末アプリの中から、指定された端末アプリを端末にインストールする。

[0022] 図1は、端末(機器1)が携帯電話10であり、ICカード(機器2)が、携帯電話10に装着されたチップ状のコンビカード20である場合の、携帯電話10、コンビカード20及びゲート40(機器3)の構成について示している。

[0023] ゲート40は、コンビカード20に対して認証処理や端末アプリの指定を行うゲートアプリ43と、コンビカード20への非接触通信を行う非接触通信手段(4)41と、ゲート40の動作を制御するCPU42とを備えている。

[0024] コンビカード20は、ゲート40への非接触通信を行う非接触通信手段(3)22と、携帯電話10への接触通信を行う接触通信手段(2)21と、認証情報等が格納された認証情報データベース(DB)25と、他の機器1、3との認証処理を行う認証アプリ24と、携帯電話10にインストールする端末アプリ27や設定命令、あるいはそれらのセットである端末アプリ・設定命令26と、コンビカード20の動作を制御するCPU23とを備えている。

[0025] また、携帯電話10は、コンビカード20への接触通信を行う接触通信手段(1)11と、携帯電話10の動作を制御するCPU12とを備えている。

[0026] このコンビカード20の認証情報DB25には、図2に示すように、ゲートアプリ43のIDと対応付けて、認証処理に使用する共通鍵や秘密鍵等の認証情報と、携帯電話10へのインストールが可能な端末アプリ27のIDや、携帯電話10で設定すべき端末アプリを指定する設定命令のIDが格納されている。

[0027] 設定命令は、例えば、携帯電話10に対する次のような指示である。・表示画面の背景イメージに会社ロゴを設定する。・音(着信時、アプリ実行時)に会社用の音を設定する。・メインメニューに、社内で使用するイントラネットアプリを追加する。・デフォルト

を内線電話に変更する(外線への発信を0発信に変更)。・メール機能の設定(メールサーバアドレス、ユーザID、個人情報、ネットワーク設定、など)を変える。・会社では特定のメールサーバにしかアクセスできない。・会社では特定のアドレスにしかメール送信できない。・会社では、特定のメールを読むことしかできない。・アクセス可能なアプリサーバを制限する。・会社では特定のサイトにしかアクセスできない。

[0028] また、携帯電話10へのインストールが可能な端末アプリは、携帯電話10で保持されていない、設定命令の実行に必要なアプリであり、例えば、以下に示すアプリがある。・設定命令に基づく表示を実行するブラウザ等のソフトウエア。例えば、会社では、特定のサイトへのアクセスのみが可能なブラウザアプのみへ切り替える。・メールアプリを切り替える。例えば、会社では、メールの保存ができない特定のメールアプリしか使えないとか、会社では会社内でないと保存したメールが閲覧できない特定のメールアプリしか使えない。例えば、保存したメールは、特定のメールアプリしかアクセスできないコンビカード20セキュアメモリエリアに保存されている。

[0029] 図3は、このゲート40、コンビカード20及び携帯電話10が連携して行う処理のシーケンスを示している。

[0030] ユーザは、所定エリアに入場する際に、コンビカード20を装着した携帯電話10をゲート40に翳す。ゲート40のCPU42は、非接触通信手段41の通信圏内にコンビカード20が進入すると、コンビカード20に認証アプリIDとゲートアプリIDとを指定して認証処理を要求する(1－1)。これを受けてコンビカード20のCPU23は認証アプリ24を起動し、認証アプリ24は、認証情報DB25のゲートアプリIDに対応する認証情報を用いて、ゲートアプリ43との間で、一般的なチャレンジレスポンスによる認証処理を実行する(1－2)。認証処理に成功すると、ゲートアプリ43は、端末アプリIDを指定して、その端末アプリの端末へのインストールを要求する(1－3)。指定する端末アプリIDは複数であっても良い。

[0031] この要求を受けたコンビカード20の認証アプリ24は、認証情報DB25の情報から、その端末アプリがインストール可能であることを確認(検証)し、その旨をCPU23に伝える。CPU23は、携帯電話10に端末アプリIDを示してインストール要求を送り(2－1)、認証アプリ24に携帯電話10との認証処理を行わせる(2－2)。なお、コンビカー

ド20を携帯電話10に装着した時点で両者間の認証処理が既に済んでいれば、この認証処理を省略しても良い。認証処理に成功すると、CPU23は、該当する端末アプリ26、27を携帯電話10に送信し(2－3)、携帯電話10のCPU12は、その端末アプリをインストールする。

[0032] このように、このゲート40、コンビカード20及び携帯電話10の間では、三者の連携により、コンビカード20とゲート40との認証の成功を条件に、コンビカード20から携帯電話10への端末アプリのインストールが実行される。そのため、このコンビカード20の動作や、携帯電話10の端末アプリを利用する処理は、ゲート40を通過して入場したエリアでのみ可能になる。

[0033] なお、ICカードの国際標準規格(接触通信に関するISO7816、非接触通信に関するISO14443)では、ICカードのカードアプリとリーダ・ライタ側の端末アプリとのデータのやり取りは、端末アプリからカードアプリに送られる「コマンド」と、カードアプリから端末アプリに送られる「レスポンス」とが基本になると規定されている。従って、国際標準規格を満たすICカードは、受動的な動作しかできず、(2－1)のインストール要求を自ら携帯電話10に送信することができない。

[0034] そのため、携帯電話10は、国際標準規格を満たすコンビカード20の場合には、ユーザが携帯電話10をゲート40に翳した時点から、非接触通信の状態を監視するためにコンビカード20にポーリング信号を送り続ける。そして、コンビカード20から非接触通信終了の応答を受けると、コンビカード20に対し、要求が有れば送信するように指示し、コンビカード20は、これに応えてインストール要求を携帯電話10に送信する(2－1)。

[0035] こうした手順を採ることにより、国際標準規格を満たすICカードにも対応することができる。

[0036] なお、ここでは、ICカードがコンビカードである場合について説明したが、ICカードが接触通信機能のみを有するときは、図4に示すように、携帯電話10の赤外線(またはBluetoothや無線LAN)等のローカル通信手段13を利用して、ICカード20とゲート40との通信を行うことができる。この場合、ゲート40が、通信手段44と携帯電話10のローカル通信手段13との通信(赤外線)接続を確立して、携帯電話10にICカー

ド20へのアクセス命令を送ると、携帯電話10はICカード20との接触通信接続を実行し、ゲート40とICカード20との通信が可能になる。ゲート40、ICカード20及び携帯電話10の三者間におけるデータのシーケンスは、図3と同じである。

[0037] また、ICカードが非接触通信機能のみを有するときには、携帯電話10およびゲート40と非接触通信を用いて通信を行う。ユーザが携帯電話10をゲート40に翳した時点から、ゲート40との処理状態を監視するために非接触ICカード20に問合せを行う。そして、非接触ICカード20は、ゲート40との処理が終了すると、携帯電話10に終了通知を返し、この結果携帯電話10は非接触ICカード20に対し、要求が有れば送信するように指示し、非接触ICカード20は、これに応えてインストール要求を携帯電話10に送信する(2－1)。または、非接触ICカード20は、ゲート40との処理が終了すると、携帯電話10に終了通知とともにインストール要求を携帯電話10に送信する(2－1)。

[0038] (第2の実施形態)

本発明の第2の実施形態では、ICカードとゲートとの認証成功を条件に、ICカードに格納されたカードアプリの利用が、端末に対して許可される場合について説明する。

ゲートは、ICカードとの認証に成功すると、ICカードに、端末での利用を許容するカードアプリのIDと、ゲートを特定するゲートPIN情報とを伝え、このカードアプリIDとゲートPINとの対情報がICカードに格納される。ICカードは、端末からカードアプリを指定して、その利用が要求されたとき、この対情報を参照して、カードアプリの利用を許可するか否かを決定する。

[0039] 図5は、この処理を連携して行う携帯電話10、コンビカード20及びゲート40の構成について示している。コンビカード20は、第1の実施形態(図1)と同様に、非接触通信手段(3)22、接触通信手段(2)21、認証情報DB25、認証アプリ24及びCPU23を備え、さらに、ゲート40との認証に成功した場合に有効になるカードアプリ28と、カードアプリIDとゲートPINとの対情報を格納するPINDB29とを備えている。また、携帯電話10は、接触通信手段(1)11、CPU12の他に、カードアプリ28を利用する端末アプリ14を備えている。ゲート40の構成は第1の実施形態(図1)と変わりが無い。

[0040] このコンビカード20の認証情報DB25には、図6に示すように、ゲートアプリ43のIDと対応付けて、認証処理に使用する認証情報と、ゲートPINの設定が可能な(即ち、ゲート40から入場したエリアで利用可能な)カードアプリのIDと、PIN設定を解除する(即ち、そのエリアで利用できなくなる)カードアプリのIDとが格納されている。

[0041] ゲート40から入場したエリアで利用可能になるカードアプリ28は、例えば、所内の内線番号電話帳アプリであり、コンビカード20とゲート40との認証が成功すると、携帯電話10の電話帳機能を実行する端末アプリ14からコンビカード20に格納された内線簿にアクセスできるようになる。

[0042] 図7は、このゲート40、コンビカード20及び携帯電話10が連携して行う処理のシーケンスを示している。

[0043] ユーザがコンビカード20を装着した携帯電話10をゲート40に翳すと、ゲート40は、コンビカード20に認証アプリIDとゲートアプリIDとを示して相互間の認証処理を要求する(1－1)。これを受けてコンビカード20の認証アプリ24は、認証情報DB25のゲートアプリIDに対応する認証情報を用いて、ゲートアプリ43との認証処理を実行する(1－2)。認証処理に成功したゲートアプリ43は、ゲートPINを設定したい(または削除したい)カードアプリのIDとゲートPINとを提示して、カードアプリIDとゲートPINとの対情報の登録(または削除)を認証アプリ24に要求する(1－3)。このときゲートアプリ43が提示するカードアプリIDの数は、複数であっても良い。

[0044] コンビカード20の認証アプリ24は、そのカードアプリIDに該当するカードアプリ28にゲートアプリIDとゲートPINとの情報を送り、確認(検証)を要求する(2－1)。カードアプリ28は、認証情報DB25を参照して、ゲートアプリとの対応関係を有しているか否か(ゲートPINの設定が可能であるか否か)を検証し、検証結果を認証アプリ24に返す(2－2)。認証アプリ24は、検証結果がOKである場合に、検証されたカードアプリIDとゲートPINとの対情報をPINDB29に格納し(2－3)、検証結果をゲートアプリ43に通知する(2－4)。以上がゲート通過時に行われる処理である。

[0045] 一方、携帯電話10の端末アプリ14がカードアプリ24を利用する場合には、次の処理が行われる。

[0046] 携帯電話10の端末アプリ14は、カードアプリIDを提示して、コンビカード20のカー

ドアプリ28にアクセスを要求する(3－1)。カードアプリ28は、認証アプリ24に、カードアプリIDを示して検証結果を要求する(3－2)。認証アプリ24は、PINDB29を参照し、そのカードアプリIDとゲートPINとの対情報が記録されているときはOKを応答し、記録されていないときはNGを応答する(3－3)。カードアプリ28は、認証アプリ24からの応答がOKである場合に、端末アプリ14に対してアクセスを許可する(3－5)。

[0047] こうした処理により、ユーザが正しいゲート40から入場した場合にのみ、カードアプリ28の利用を可能にすることができ、例えば、ユーザがコンビカード20等のICカードを装着した携帯電話10を正規のゲート40に翳してオフィスに入場すると、ICカードに格納されたオフィス用の内線番号電話帳アプリが自動的に有効になる。

[0048] なお、ゲートアプリ43から提示されたカードアプリIDがPIN設定を解除するカードアプリIDとして認証情報DB25に記録されている場合には、認証アプリ24は、PINDB29を参照し、そこに記録されているカードアプリIDとゲートPINとの対情報を削除する。

[0049] このようにPINDB29の削除処理を併せて行うことにより、例えば、ユーザが、入門処理をして、あるオフィスに入場した後、別のオフィスに入門処理をして入場した場合に、先のオフィス用の内線番号電話帳アプリが無効になり、後から入場したオフィス用の内線番号電話帳アプリだけが有効になる。

[0050] なお、各処理のメッセージ及びデータは、第三者の盗聴を防ぐために暗号化して送信するようにしても良い。

[0051] また、図7において、(2－3)の検証結果の格納は、カードアプリIDの検証結果がOKであることを示す情報だけをPINDB29に格納するようにしても良い。

[0052] また、コンビカード20等のICカードは、接触通信機能のみを有するものであっても良い。この場合には、第1の実施形態(図4)で説明したように、携帯電話10のローカル通信手段を利用してICカードとゲートとの通信を行う。また、ICカードは、非接触通信機能のみを有するものであっても良い。

[0053] なお、図6に示す認証情報DB25において、一つのゲートアプリIDに対し、複数のカードアプリIDが設定されている場合には、端末アプリ14のアクセスを許容するカー

ドアプリに優先度を設定することも可能である。この場合、図8に示すように、ゲートアプリIDに対応して、優先度設定可能なカードアプリID及び優先度設定を解除できるカードアプリIDの優先度を設定した優先設定DBを保持する。あるいは、図9Aに示すように、各カードアプリIDの優先度を優先度テンプレートで規定し、図9Bに示すようにゲートアプリIDに対応して優先度テンプレートを設定した優先設定DBを保持する。

[0054] そして、認証情報DB25から、ゲートアプリIDに対応するカードアプリ28を選択する場合に、優先設定DBを参照し、優先度に基づいて選択するカードアプリ28を決定する。

[0055] (第3の実施形態)

本発明の第3の実施形態では、ICカードとゲートとの認証成功を条件に、ICカードに格納されたカードアプリの利用が、端末に対して許可される第2の実施形態の構成において、ICカード、ゲート及び端末の三者間での処理が、第2の実施形態と異なる手順で行われる場合について説明する。

[0056] ここでは、図10に示すように、機器1が、非接触通信手段(1)110を有するドア100であり、機器2が、非接触通信手段22のみを有するICカード200であるものとして説明する。機器1、機器2及び機器3のその他の構成は、第2の実施形態(図5)と変わりがない。

ここでは、非接触通信手段22のみを有するが、接触通信手段のみを有しても良い。

[0057] 図11は、ゲート40、ICカード200及びドア100が連携して行う処理のシーケンスを示している。

[0058] ユーザがICカード200をゲート40に翳すと、ゲート40は、ICカード200に認証アプリIDとゲートアプリIDとを示して相互間の認証処理を要求する(1－1)。これを受けてICカード200の認証アプリ24は、認証情報DB25のゲートアプリIDに対応する認証情報を用いて、ゲートアプリ43との認証処理を実行する(1－2)。認証処理に成功したゲートアプリ43は、ゲートPINを設定するカードアプリのIDとゲートPINとを提示して、カードアプリIDとゲートPINとの対情報の登録を認証アプリ24に要求し(1－3)、

ICカード200の認証アプリ24は、要求に従ってカードアプリIDとゲートPINとの対情報をPINDB29に登録する(1－4)。この登録の段階では、認証情報DB25との検証は済んでいない。以上がゲート通過時に行われる処理である。

[0059] 一方、ユーザがICカード200をドア100に翳すと、次の処理が行われる。

[0060] ドア100の端末アプリ14は、端末アプリIDとカードアプリIDとを提示して、ICカード200のカードアプリ28へのアクセスを要求する(2－1)。カードアプリ28は、認証アプリ24に、カードアプリIDとゲートアプリIDとを示してPINDB29の登録情報を要求し(2－2)、認証アプリ24は、PINDB29から、該当するカードアプリID及びゲートPINの対情報を取得してカードアプリ28に提示する(2－3)。カードアプリ28は、認証情報DB25を参照して、ゲートアプリとの対応関係を有しているか(ゲートPINの設定が可能であるか)を検証し(2－4)、検証結果がOKである場合に、端末アプリ14にアクセスを許可する(2－5)。

[0061] カードアプリ28にアクセスしたドア100の端末アプリ14は、例えば、カードアプリ28から鍵情報を取得してドア100を開錠し、ユーザは、ドア100の通過が可能になる。

[0062] このように、ゲート40、ICカード200及びドア100が連携することにより、正しい玄関(ゲート)から入らないと、ドアが開かないようにすることができる。

[0063] また、このPIN検証(2－4)では、カードアプリ28が、端末アプリ14とゲートPINとのペアを検証することも可能であり、この場合には、ある端末アプリ14について、特定のゲートPINと対応していなければアクセスを許可しない(即ち、あるドアは特定の入口から入らないと開かない)と言う制御を行うこともできる。

[0064] また、図12に示すように、ドア100にPIN入力部15を設け、ユーザがPIN入力部15から入力したユーザPINをさらに検証して、ドア100を開けるように制御することもできる。

[0065] 図13は、この場合のシーケンスを示している。ゲートPINを検証する(2－4)までの処理は、図11の場合と同じである。ゲートPINの検証結果がOKである場合に、カードアプリ28は、ドア100にユーザPINを要求し(2－5)、ユーザがPIN入力部15からユーザPINを入力すると(2－6)、カードアプリ28は、ICカード200のPINDB29で保持されたユーザPINと照合して、それを検証する(2－7)。そして、検証結果が一

致する場合に、端末アプリ14に対してアクセスを許可する(2－8)。

[0066] (第4の実施形態)

本発明の第4の実施形態では、ICカードとゲートとの認証処理が成功したことを条件に、機器の処理が可能になる場合について説明する。

[0067] ICカードは、ゲートとの認証処理が成功すると、ゲートからゲートPINを取得し、このゲートPINを機器に送信する。機器は、ゲートPINの検証が終了した後、処理を開始する。

[0068] 図14は、ゲート40、コンビカード20及び携帯電話10の構成と、機器(機器4)が金庫50である場合の構成とを示している。このコンビカード20を装着した携帯電話10をゲート40に翳し、コンビカード20とゲート40との認証処理を行う。認証が成功した場合に、この携帯電話10を金庫50に翳し、また、携帯電話10からユーザPINを入力することにより、金庫50の開錠が可能になる。

[0069] 金庫50は、コンビカード20への非接触通信を行う非接触通信手段(5)51と、金庫50の鍵の開閉を制御する鍵アプリ53と、金庫50の動作を制御するCPU52とを備えている。ゲート40、コンビカード20及び携帯電話10の構成は、第2の実施形態(図10)と変わりがない。

[0070] コンビカード20を装着した携帯電話10をゲート40に翳すと、ゲート40とコンビカード20との間で、図13の(1－1)から(1－4)までの処理が行われる。

[0071] 図15は、その後、ユーザが、コンビカード20を装着した携帯電話10を金庫50に翳したときの処理シーケンスを示している。

[0072] 金庫50の鍵アプリ53は、カードアプリIDを示して、コンビカード20にカードアプリ29へのアクセスを要求する(3－1)。カードアプリ29は、カードアプリID及び鍵アプリIDを提示して、認証アプリ24にゲートPINを要求する(3－2)。認証アプリ24は、PIN DB29を参照し、カードアプリIDに対応するゲートPIN情報を取得してカードアプリ29に返す(3－3)。

[0073] 次に、カードアプリ29は、携帯電話10の端末アプリ14にユーザPINを要求する(3－4)。端末アプリ14は、PIN入力画面を表示し、ユーザがPINを入力すると(3－5)、そのユーザPINをカードアプリ29に送信する(3－6)。カードアプリ29は、コンビカ

ード20のPINDB29で保持されているユーザPIN情報と照合して、それを検証する(3－7)。ユーザPINの検証結果が一致した場合は、ゲートPINを金庫の鍵アプリ53に送信する(3－8)。鍵アプリ53は、予め保持するゲートPIN情報と、カードアプリ29から送られたゲートPINとを照合して検証し(3－9)、検証結果が一致する場合に、開錠処理を実行する(3－10)。

[0074] このように、例えば、ゲート40が玄関に設置されている場合では、玄関での入門処理が正しく行われたときにのみ、金庫50の鍵が使えることになる。

[0075] なお、ユーザPINやゲートPINの検証を行う時期、あるいは、検証を行う主体等については、種々の変更が可能である。例えば、鍵アプリ53がゲートPINの検証(3－9)を行う代わりに、カードアプリ29が、ユーザPIN検証(3－8)とともに、ゲートPINの検証を行い、検証結果を鍵アプリ53に伝えるようにしても良い。

[0076] また、カードアプリ29がユーザPIN検証(3－8)を行う代わりに、入力されたユーザPINを鍵アプリ53に送り、鍵アプリ53が、金庫50に登録されたユーザPINと照合してユーザPIN検証を行うようにしても良い。

[0077] また、図16に示すように、PIN登録(4－4)を終了した認証アプリ24が、端末アプリ14にユーザPINを要求し(4－5)、入力されたユーザPINをそのままPINDB29に登録(4－8)するようにしても良い。この場合は、図17に示すように、携帯電話10を金庫50に翳した段階で、カードアプリ29が、PINDB29からゲートPIN及びユーザPINを取得し(5－3)、ユーザPINを検証し(5－4)、ゲートPINを金庫50の鍵アプリ53に送る(5－5)。この方式では、ユーザのPIN入力が事前に済んでいるため、金庫50の前でのユーザの入力操作が不要になる。

[0078] また、図18に示すように、PIN登録(4－4)が終了した時点で、認証アプリ24がPIN登録通知(ゲートアプリID)をカードアプリ29に対し行ない(4－5)、その通知を受けたカードアプリ28が、携帯電話10に対しカードアプリIDを渡しながらユーザPINを要求する(4－6)。携帯電話10の端末アプリ14は、ユーザPINを入力し(4－7)、ユーザPINをコンビカード20のカードアプリ28に対し送信する。コンビカード20では、カードアプリ28が入力されたユーザPINを検証して(4－9)、ユーザPINの認証結果を認証アプリ24に送信する。認証アプリ24では、カードアプリ28からのユーザPINの

検証結果を登録する(4－11)ようにしてもよい。この場合は、図19に示すように、携帯電話10を金庫50に翳した段階で、ユーザの検証結果をチェックする(5－4)だけで足りる。この方式では、ユーザPIN検証が早い段階で行われるため、ユーザがPIN入力を間違えていた場合に、早い段階で修正できる。

[0079] また、図20は、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN要求と、ゲートPIN検証と、ユーザPIN検証とを行う場合のシーケンスを示している。

[0080] また、図21は、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN要求と、ユーザPIN検証とを行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証を行う場合のシーケンスを示している。

[0081] また、図22は、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN要求と、ゲートPIN検証とを行い、金庫(機器4)の鍵アプリ(アプリ5)がユーザPIN検証を行う場合のシーケンスを示している。

[0082] また、図23は、コンビカード(機器2)の認証アプリ(アプリ3)が、ユーザPIN要求を行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証と、ユーザPIN検証とを行う場合のシーケンスを示している。

[0083] また、図24は、ユーザPIN入力を金庫(機器4)から行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証と、ユーザPIN検証とを行う場合のシーケンスを示している。

[0084] また、図25は、ユーザPIN入力を金庫(機器4)から行い、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN検証を行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証を行う場合のシーケンスを示している。

[0085] また、図26は、ユーザPIN入力を金庫(機器4)から行い、コンビカード(機器2)のカードアプリ(アプリ2)が、ゲートPIN検証を行い、金庫(機器4)の鍵アプリ(アプリ5)がユーザPIN検証を行う場合のシーケンスを示している。

[0086] コンビカード(機器2)のカードアプリ(アプリ2)でゲートPINを検証する場合は、ゲートPINが変わった場合に、カード内に格納されたゲートPINを変更すれば足りる。また、ゲートアプリ(アプリ4)と鍵アプリ(アプリ5)の組み合わせでアクセス制御を行うことができる。

[0087] また、金庫(機器4)の鍵アプリ(アプリ5)でゲートPINを検証する場合は、新しい金庫(機器4)が追加された時に、その金庫にゲートPIN情報を登録するだけで足りる。また、金庫を削除するときに、カードの設定を変える必要がない。

[0088] また、コンビカード(機器2)のカードアプリ(アプリ2)でユーザPINを検証する場合は、ユーザがユーザPINを変えたい場合に、コンビカード(機器2)に格納されているユーザPINを変更するだけで足り、わざわざユーザPINを換えたい機器(例えば金庫)のところに赴いて変えなくても済む。また、一つのユーザPINが複数の機器(ドアなど)に対応している場合でも、ドアごとにユーザPINを設定して回らなくて済む。また、図18に示すように、ユーザPINを事前入力する場合に、ユーザPINの入力時に金庫(機器4)無しで検証が行えるので、金庫に翳してからユーザPINの再入力が必要になるような事態は発生しない。

[0089] また、金庫(機器4)の鍵アプリ(アプリ5)でユーザPINを検証する場合は、金庫でユーザPINを管理しているので、何人のユーザが登録されているのかが容易に把握できる。

[0090] また、本実施形態では、機器4を金庫、カードアプリとして鍵アプリを想定したが、機器4をビデオやセットトップボックス(STB)、カードアプリとして、決済カードアプリや、有料放送録画予約アプリ、有料放送受信操作アプリを想定してもよい。こうすることにより、正しく玄関の鍵の処理をしていないと、STB(PC)を介した決済処理(決済カードアプリ)ができない、ビデオ録画予約(その解除)(有料放送録画アプリ)ができない、といったサービスも可能である。

[0091] また、機器4を車の防犯モジュールとした場合、正しく玄関の鍵を閉じる処理をしたカードアプリと防犯モジュール(機器4)で正しいチェックイン処理をしないまま、車のドアを開けたり、車のエンジンをかけたり、車のオーディオを外したりすると防犯ベルが鳴るといったサービスも可能である。

[0092] なお、実施形態では、主に、ICカードを携帯電話に装着する場合について説明したが、本発明はこれに限定されるものではない。携帯電話に代えて、PDA(Personal Digital Assistant)、メール端末、小型パーソナルコンピュータ、ゲーム機など、各種の端末装置・情報処理装置を用いることができる。また、ICカードは、国際標準規格を

満たすものでも、満たさないものでも使用可能である。セキュアデバイスの形状は、カード状でもチップ状でも良く、情報処理装置に埋め込む形態であっても良い。また、ICカードは接触通信手段のみを有しても良い。

[0093] (第5の実施形態)

次に、本発明の第5の実施形態について説明する。第5の実施形態は、通信方式に応じてインストール可能なあるいは削除する端末アプリおよび設定命令の設定を変えるようにしたものである。なお、構成自体は、図1に示す実施形態1のものと同じであるので、図1を参照して説明する。

[0094] 図1に示すように、第5の実施形態でも、第1の実施形態と同様に、端末(機器1)である携帯電話10と、ICカード(機器2)である携帯電話10に装着されたチップ状のコンビカード20と、ゲート機器(機器3)であるゲート40から構成されている。

[0095] そして、第5の実施形態の場合、ICカード(機器2)であるコンビカード20が複数通信方式に対応した近距離無線通信機能を有する非接触通信手段22を有しており、通信方式によってンストール可能なあるいは削除する端末アプリおよび設定命令の設定を変えるようにしている。

[0096] ここでは、一例として、会社の入場処理と退場処理とで、異なる通信方式を用いて端末アプリおよび設定命令の設定を変える例について説明する。

[0097] 図27は、第5の実施形態における会社の入場処理と退場処理とを例にした認証情報DB25の一例を示す。

[0098] 図27の例では、通信方式としてISO14443typeA等の独自通信方式Aと、ISO14443typeB等の独自通信方式Bとの2つがあり、独自通信方式Aの場合、インストール可能な端末アプリIDとして端末アプリ1ID(個人用メーラ)および端末アプリ2ID(ゲーム)、インストール可能な設定命令IDとして個人のネットワーク設定や、壁紙、通常通話モード等の設定命令5ID、削除する端末アプリIDとして端末アプリ3ID(内線番号閲覧ブラウザ)、削除する設定命令IDとして(会社用設定である会社のネットワーク設定、壁紙、内線モード等の設定命令7IDがあることを示している。

[0099] また、独自通信方式Bの場合、インストール可能な端末アプリIDとして端末アプリ1ID(会社用メーラ)および端末アプリ3ID(内線番号閲覧ブラウザ)があり、インストール

可能な設定命令IDとして設定命令7ID(会社用設定: 会社のネットワーク設定、壁紙、内線モード)、削除する端末アプリIDとして端末アプリ1ID(個人用メーラ)および端末アプリ2ID(ゲーム)、削除する設定命令IDとして設定命令5ID(個人のネットワーク設定、壁紙、通常通話モード)があるものとする。

[0100] これにより、同一のゲートアプリ43から命令が来ても、あるいはアプリIDにかかわらず、通信方式に応じて、設定を変更することができる。

[0101] 例えば、図27の例では、例えば、DBテーブルのID1が出口、ID2が入り口の処理とする。ID1の入り口と、ID2の出口とでは、ゲートアプリIDは同じだが、通信方式が独自通信方式Aと、独自通信方式Bとで異なるものとする。なお、ゲートアプリIDはなくてもよく、ゲートアプリIDでなく、ゲート機器IDでもよい。

[0102] この例の場合、個人用アプリとして、個人用メーラ(アプリ1)、ゲーム(アプリ2)、会社用アプリとして、会社用メーラ(アプリ4)、コンビカード20内に格納された内線番号データにアクセスできる内線電話番号閲覧ブラウザ(アプリ3)があり、入口(2)と、出口(1)で削除またインストールされる。

[0103] また、設定命令も、会社用、個人用があり、例えば、アクセス可能なネットワークの設定や、壁紙、通話モードなどが切り替えられる。

[0104] 次に図を参照して動作を説明する。

[0105] 図28は、第5の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図である。

[0106] 本実施形態の場合、機器2であるコンビカード20の非接触通信手段(3)22が、機器3であるゲート40の非接触通信手段(4)41と非接触通信を行い、機器3であるゲート40から機器2であるコンビカード20に対し、処理要求が送信された場合(6－1)、コンビカード20のCPU23は、その非接触通信の通信方式を検出し(6－2)、機器3であるゲート40との間で認証処理を行い(6－3)、認証情報DB25の認証情報を参照して認証処理を確認する(6－4)。

[0107] コンビカード20のCPU23は、認証処理が確認できた場合、機器3であるゲート40に対し、認証した処理を通知する(6－5)。これにより、ゲート40では、機器2であるコンビカード20に対しインストールするアプリや設定命令を確認することができる。なお

、この通知は、省略しても勿論よい。そして、ゲート40は、その処理通知を受けて、通信方式に応じてゲートアプリ43に対応したゲートを開く(6－6)。

[0108] 一方、コンビカード20のCPU23は、接触通信手段(2)21を介し、機器1である携帯電話10に対し、検出した通信方式に応じて、インストール可能なあるいは削除する端末アプリIDおよび設定命令IDの設定要求を送信し(6－7)、認証処理を行う(6－8)。

[0109] そして、認証できた場合には、コンビカード20のCPU23は、接触通信手段(2)21を介し、機器1である携帯電話10に対し、検出した通信方式に応じて、インストール可能なあるいは削除する端末アプリIDおよび設定命令IDを送信し(6－9)、携帯電話10では、コンビカード20とゲート40との間の通信方式に応じたインストール可能なあるいは削除する端末アプリIDおよび設定命令IDを、機器2のCPU23からの指示に従いインストールまたは削除し(6－10)、その結果をコンビカード20へ通知する(6－11)。

[0110] これにより、携帯電話10へは、コンビカード20とゲート40との間の通信方式に応じた端末アプリIDおよび設定命令IDをインストールしたり、あるいは通信方式に応じて削除することが可能となる。

[0111] なお、コンビカード20と機器1である携帯電話10との間の認証処理は、インストール可能なあるいは削除する端末アプリIDおよび設定命令IDの設定要求の前に行っても良い。また、コンビカード20と機器1である携帯電話10に装着した時点で認証処理する場合には、コンビカード20と携帯電話10との間の認証処理は、不要となる。

[0112] このように、第5の実施形態によれば、通信方式に応じて、携帯電話10にインストールや、携帯電話10から削除する端末アプリや設定命令を変更することにより、場所だけでなく、通信方式に応じても、携帯電話10の機能を変更することができる。

[0113] なお、本実施形態では、通信方式に応じてインストール可能なあるいは削除する端末アプリおよび設定命令の設定を変える機能をCPU23に持たせているが、認証アプリ24にこのような機能を持たせるようにしても勿論良い。

[0114] (第6の実施形態)

次に、本発明の第6の実施形態について説明する。第6の実施形態は、通信方式

に応じて有効および無効(使用禁止)にするカードアプリを変えるようにしたものである。なお、構成自体は、カードアプリを使用する図5に示す第2の実施形態や、図10に示す第3の実施形態、図12に示す第3の実施形態のものと同じであるので、図1を参照して説明する。

[0115] 機器2であるコンビカード20が、複数の近距離無線通信機能を有する非接触通信手段(3)22を有する場合、通信方式によってカードアプリの有効または無効を変えることができる。ここで、カードアプリを無効にする、とは、例えば、R/W(リードライタ)からICカードにISO7816規格のセレクトコマンドを送っても、ICカードから応答を返さない状態をいう。

[0116] ここで、近距離無線によって、用途が限定される場合がある。例えば、ISO14443タイプAは金融用途、ISO14443タイプBは公共向け用途、JICSAP2.0は交通向け等の特定エリア用途などと限定されている。

[0117] このように、通信方式に応じて携帯電話10の端末アプリ14からコンビカード20のカードアプリ28へのアクセスを制限することで、ユーザが分野外のどのカードアプリ28を格納しているかゲート40等のR/W(リードライタ)に分からないようにする。例えば、カードアプリIDは公知なものなので、どのR/W(リードライタ)でも、ISO7816規格のセレクトコマンドを送ると、コンビカード20等のICカードからの応答でカードアプリの有無が分かってしまう。

[0118] つまり、公共のサービス用のR/W(リードライタ)が、そのユーザがどんなクレジットカードアプリをもっているかという個人情報を、ユーザに知られずに取得することが可能となる。

[0119] そこで、この第6の実施形態では、通信方式に応じて、無効、すなわち使用禁止にするアプリIDを設定できるようにしたものである。

[0120] 図29は、第6の実施形態の認証情報DB25の内容の一例を示す図である。

[0121] 図29において、通信方式がISO14443typeBの場合、無効にするアプリIDはカードアプリ3ID(クレジットカード)、通信方式がISO14443typeAの場合、無効にするアプリIDはカードアプリ1ID(運転免許証)、通信方式がJICSAP2.0の高速コマンド仕様の場合、無効にするアプリIDはカードアプリ3ID(クレジットカード)であるとする。

[0122] 次に図を参照して動作を説明する。

[0123] 図30は、第6の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図である。

[0124] 本実施形態の場合、機器2であるコンビカード20の非接触通信手段(3)22が、機器3であるゲート40の非接触通信手段(4)41と非接触通信を行い、機器3であるゲート40から機器2であるコンビカード20に対し、リクエストコマンドが送信された場合(7－1)、コンビカード20のCPU23は、その非接触通信の通信方式を検出し(7－2)、通信方式を検出できた場合、応答コマンドを返す(7－3)。

[0125] そして、機器3であるゲート40からカードアプリのセレクトコマンドが送信された場合には(7－4)、コンビカード20のCPU23は、認証情報DB25を参照してアクセス可否を確認し(7－5)、セレクトコマンド応答を、機器3であるゲート40に対し返す(7－6)。

[0126] つまり、コンビカード20のCPU23は、認証情報DB25に格納された図29の認証情報を参照し、ゲート40から指定されたカードアプリIDが、コンビカード20とゲート40との間の通信方式に対応した無効にするアプリIDに指定されていなければ正常応答を返し、指定されていればエラー応答を、セレクトコマンド応答とし、ゲート40に対し返すようにする。

[0127] 例えば、コンビカード20とゲート40との間の通信方式がISO14443typeBであり、ゲート40から指定されたカードアプリIDが、カードアプリ3ID(クレジットカード)の場合は、図29に示す認証情報DB25の内容を参照すると、無効にするアプリIDであるため、コンビカード20はゲート40に対し、セレクトコマンド応答としてエラー応答を返す。通信方式がJICSAP2.0の高速コマンド仕様の場合も同様である。

[0128] これに対し、コンビカード20とゲート40との間の通信方式がISO14443typeBであり、ゲート40から指定されたカードアプリIDが、カードアプリ1ID(運転免許証)の場合は、図29に示す認証情報DB25の内容を参照すると、無効にするアプリIDには該当しないため、コンビカード20はゲート40に対し、セレクトコマンド応答として正常応答を返す。

[0129] これにより、コンビカード20とゲート40との間の通信方式に応じて有効および無効(

使用禁止）にするカードアプリ28が変わるので、携帯電話10の端末アプリ14は、コンビカード20とゲート40との間の通信方式に応じて、コンビカード20におけるカードアプリ20にアクセスできる場合と、アクセスできない場合とが生じることになる。

[0130] このように、第6の実施形態によれば、コンビカード20とゲート40との間の通信方式に応じてコンビカード20内の端末アプリ27の無効にするアプリIDを設定できるようにしたため、通信方式に応じてコンビカード20等のICカードへのアクセス制限をすることで、ユーザが分野外のどのアプリを格納しているかゲート40等のR／W（リードライタ）に分からないようにすることができる。

[0131] なお、この第6の実施形態では、通信方式に応じて無効にするアプリIDを指定するように説明したが、この第6の実施形態と、前述の第5の実施形態とを組み合わせて、機器2であるコンビカード20と、機器3であるゲート40との間の1回の通信方式の検出および認証処理により、通信方式に応じて、インストールまたは削除する端末アプリIDおよび設定命令ID、および無効にするアプリIDを同時に変えるようにしても勿論よい。

[0132] また、この第6の実施形態では、機器2であるコンビカード20のCPU23にコンビカード20とゲート40との間の通信方式に応じてコンビカード20内の端末アプリ27の無効にするアプリIDを設定する機能を持たせたが、コンビカード20の認証アプリ24等にかかる機能を持たせても勿論良い。

[0133] （第7の実施形態）

次に、本発明の第7の実施形態について説明する。第7の実施形態は、前回、機器2であるコンビカード20と機器1である携帯電話10との間で有効にした設定が正しく無効化されていれば、今回、機器3であるゲート40と、機器2であるコンビカード20との認証を許可するようにしたものである。

[0134] 図31は、第7の実施形態の構成を示すブロック図である。

[0135] この第7の実施形態では、機器2であるコンビカード20に端末設定管理部210を設け、端末設定管理部210により前回の機器1である携帯電話10と機器2であるコンビカード20で有効にした設定が、正しく無効化されていれば、今回、機器3であるゲート40と機器2であるコンビカード20との間の認証を許可するようにしたものである。な

お、端末設定管理部210は、認証アプリ24と一体でも勿論よいし、CPU23と一体でも勿論よい。その他の構成は、図1に示す実施形態1等のものと同じであるので、図1の構成と同一符号を付して説明を省略する。

[0136] 図32に、第7の実施形態の認証情報DB25に設定されたデータの一例を示す。

[0137] 認証情報DB25には、ID1、ID2それぞれのデータが設定されている。

[0138] ID1の場合、www.app.co.JP/gate1、通信方式はISO14443typeB、有効時間は5;00時間、インストール可能な端末アプリIDおよび設定命令IDとして端末アプリ3ID(内線番号閲覧ブラウザ)および設定命令7ID(会社用設定: 会社のネットワーク設定、壁紙、内線モード)、削除する端末アプリIDおよび設定命令IDとして端末アプリ2ID(ゲーム)および設定命令5ID(個人のネットワーク設定、壁紙、通常通話モード)が設定されている。

[0139] また、ID2の場合、www. app. co. JP／gate2、通信方式はUWB(Ultra WIDe Band)、有効時間は制限なし、インストール可能な端末アプリIDおよび設定命令IDとして端末アプリ2ID(ゲーム)および設定命令5ID(個人のネットワーク設定、壁紙、通常通話モード)、削除する端末アプリIDおよび設定命令IDとして端末アプリ3ID(内線番号閲覧ブラウザ)および設定命令7ID(会社用設定: 会社のネットワーク設定、壁紙、内線モード)が設定されている。

[0140] 図33に、第7の実施形態の端末設定管理部210に設定されたデータの一例を示す。

[0141] 端末設定管理部210に設定されたデータでは、ID1として、機器3のIDがwww. app. co. jp／gateterminal1、ゲートアプリIDがwww. app. co. jp／gateapp1、機器1のIDがwww. app. co. jp／terminal1、設定時のタイムスタンプが2004／12／24 15:32:02、有効時間が5:00時間、認証情報DB25のIDが1、インストールした時の端末アプリIDが端末アプリ3ID(内線番号閲覧ブラウザ)、インストールした設定命令IDが設定命令7ID (会社用設定: 会社のネットワーク設定、壁紙、内線モード)、削除した端末アプリIDが端末アプリ2ID(ゲーム)、削除した設定命令IDが設定命令5ID(個人のネットワーク設定、壁紙、通常通話モード)、設定処理結果が正常である、等のデータが、認証アプリ24から端末設定管理部210への設定通知処理に

より格納される(図34の8－14)。

[0142] それ以外に、端末設定管理部210に設定されたデータでは、図33に示すように、復活通知時のタイムスタンプとして2004／12／24 20:32:02、復活処理結果として正常が、機器1のCPU12から機器2の認証アプリ24への復活通知結果に基づく認証アプリ24から端末設定管理部210への復活結果通知処理により格納される(図34の8－20)。

[0143] 次に図を参照して動作を説明する。

[0144] 図34は、第7の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図である。

[0145] まず、インストール時の処理から説明すると、本実施形態の場合、機器2であるコンビカード20の非接触通信手段(3)22が、機器3であるゲート40の非接触通信手段(4)41と非接触通信を行い、機器3であるゲート40のゲートアプリ43から機器2であるコンビカード20の認証アプリ24に対し、認証要求が送信された場合(8－1)、コンビカード20の認証アプリ24は、機器3であるゲート40との間で認証処理を行う(8－2)。

[0146] そして、認証処理がOKであった場合、コンビカード20の認証アプリ24は、前回の結果を端末設定管理部210に対し要求し(8－3)、端末設定管理部210は、前回の結果がOKであれば、認証アプリ24に対し前回結果OKを返す(8－4)。

[0147] すると、認証アプリ24は、ゲート40のゲートアプリ43に対し、前回結果OKを通知して(8－5)、ゲート40のゲートアプリ43は、ゲートをオープンにする(8－6)。なお、機器2であるコンビカード20と、機器3であるゲート40との間の非接触通信での認証時に前回の端末設定の結果を取得した際、前回有効にした設定が正しく無効化されていない場合は、認証を許可しないようにする。

[0148] また、コンビカード20の認証アプリ24は、前回結果OKの場合、機器1である携帯端末10に対しインストール要求を送信し(8－7)、携帯端末10のCPU12との間で認証処理を実行する(8－8)。

[0149] 認証処理がOKの場合、コンビカード20の認証アプリ24は、機器1である携帯端末10に対し、端末アプリ27を送信し(8－9)、携帯端末10はその端末アプリ27を受信

してインストールする(8－10)。

[0150] そして、携帯端末10のCPU12は、コンビカード20から受信した端末アプリ27がインストールできた場合は、インストール結果OKの通知をコンビカード20の認証アプリ24に対し行ない(8－11)、認証アプリ24は、端末設定管理部210に対し設定通知を行なう(8－13)。

[0151] 端末設定管理部210は、認証アプリ24からの設定通知により、図33に示すID、機器3のID、ゲートアプリID、機器1のID、設定時のタイムスタンプ、有効時間、認証情報DBのID、インストールした時の端末アプリID、インストールした設定命令ID、削除した設定命令ID、設定処理結果を格納し(8－14)、かかるデータの格納後、格納結果OKの通知を認証アプリ24に対し行う(8－15)。

[0152] 一方、携帯端末10では、ンストール結果OKの通知をコンビカード20の認証アプリ24に対し行なった(8－11)後、タイマー管理を行う(8－16)。ここで、このタイマー管理を行う代わりに、コンビカード20の端末設定管理部210が認証アプリ24に対し格納結果を通知(8－15)した後に、認証アプリ24がタイマー管理を行い、後述する機器1の携帯端末10における復活処理(8－17)の前に機器2の認証アプリ24から機器1のCPU12に対し復活命令を行うようにしても良い。これで、インストール時の処理が終了する。

[0153] 一方、復活時の処理は、機器1である携帯端末10にて、復活処理、すなわちインストールした端末アプリ・設定命令の削除処理を行った場合(8－17)、携帯端末10のCPU12は、復活結果OKの通知をコンビカード20の認証アプリ24に対し行う(8－18)。

[0154] ここで、復活時の処理の際、インストールされた端末アプリを削除するが、例えば、有効時間内に出口処理をした場合などは、インストールされた端末アプリがすでに削除されている場合もある。このような場合にも、復活結果OK、もしくは削除済みをコンビカード20の認証アプリ24に対し行うようにする。

[0155] 機器2であるコンビカード20の認証アプリ24は、携帯端末10のCPU12からの復活結果OKの通知を受けて、復活結果通知を端末設定管理部210へ送信する(8－19)。

[0156] 端末設定管理部210では、認証アプリ19からの復活結果通知を受けると、例えば、図33に示す復活通知時のタイムスタンプ、および復活処理結果を認証情報に格納し(8－20)、格納結果OKであれば、その格納結果OKを認証アプリ24に通知する(8－21)。

[0157] なお、よりセキュアにするためには、携帯端末10のCPU12から機器2であるコンビカード20の認証アプリ24に対する復活結果OKの通知処理(8－18)の前か後ろに認証処理を入れるようにしても勿論良い。

[0158] このように、第7の実施形態によれば、前回、機器2であるコンビカード20と機器1である携帯電話10との間で有効にした設定が正しく無効化されていれば、今回、機器3であるゲート40と、機器2であるコンビカード20との認証を許可する一方、前回、機器2であるコンビカード20と機器1である携帯電話10との間で有効にした設定が正しく無効化されていない場合には、今回、機器3であるゲート40と機器2であるコンビカード20との認証を許可しないようにしたので、毎回、毎回、機器1と機器2との間で有効にした設定が正しく無効にしたかを確認してから、機器3と機器2との認証を許可することができ、よりセキュリティを向上させることができる。

[0159] また、この第7の実施形態では、端末設定管理部210は、前回の端末設定の結果を管理する際、設定した内容である設定命令やインストールを認証情報に格納すると共に、有効時間後に削除(無効化)命令を出して削除を確認すると共に、端末1である携帯端末10がタイマー管理しているその有効時間に基づいて削除管理通知を受け付け、前回の設定である図33に示す設定内容等を履歴として認証情報に格納するようにしたので、次回ゲート認証時にその認証情報を参照することにより確実に前回の履歴を提供することができる。

[0160] なお、この第7の実施形態では、認証アプリ24とは別に、端末設定管理部210を設けて説明したが、端末設定管理部210は、認証アプリ24と一体、すなわちその一機能として設けたり、さらにはCPU23と一体、すなわちその一機能として設けるようにしても勿論よい。

[0161] (第8の実施形態)

次に、本発明の第8の実施形態について説明する。第8の実施形態は、機器1であ

る携帯電話のメモリ容量確保等のため、携帯電話の端末アプリを退避させた場合、機器2であるコンビカードがその端末アプリを関して、設定解除処理の際に、インストールし直すようにしたものである。

[0162] 図35は、第8の実施形態の構成を示すブロック図である。

[0163] 図35において、第8の実施形態の場合、機器1である携帯電話10は、携帯電話10における端末アプリの退避を管理する端末アプリ退避管理部120をさらに有している。また、機器2であるコンビカード20は、携帯電話10における端末アプリの退避を管理した際の端末の設定を管理する端末設定管理部220をさらに有している。なお、その他の構成は、図1などに示すものと同じであるので、同一符号を付してその説明は省略する。

[0164] つまり、この第8の実施形態では、携帯電話10からの端末アプリの退避する場合は、機器2であるコンビカード20からインストール要求受信時に、携帯電話10の端末メモリ(図示せず)の容量が少なく、新たに端末アプリ27をインストールできない場合は、端末設定管理部220と、端末アプリ退避管理部120とで、認証を行う。そして、その認証に成功すれば、携帯電話10がインストールしている端末アプリと、その端末アプリが保持するデータとを、端末設定管理部220が機器1の端末アプリ退避管理部120からしかアクセスできないセキュアな領域、例えば、ICカード20のタンパ領域またはICカード20の暗号化されたフラッシュメモリ領域などに格納する。また、認証時に鍵生成を行い、その鍵情報に基づいて暗号化して保存してもよい。

[0165] 機器1である携帯電話10にて退避する端末アプリの選択方法は、機器1で端末アプリに優先順位をつけて保持しておく、あるいは機器2であるコンビカード20から例えば、インストール要求に含めて退避するアプリを指定する等がある。

[0166] 一方、復活時は、機器2であるコンビカード20から設定解除命令時に、コンビカード20に退避されたアプリがあれば、設定解除処理確認後に、退避された端末アプリの復活命令を送り復活のための認証処理を行わせる。そして、端末設定管理部220と端末アプリ退避管理部120との間で認証を行い、その認証が成功すれば、退避された端末アプリと、そのデータとを端末アプリ退避管理部120に送信し、端末アプリ退避管理部120がその端末アプリの再インストール、端末アプリデータのリストアを行う

[0167] なお、この第8の実施形態においても、前述の第7の実施形態と同様に、機器2であるコンビカード20と、機器3であるゲートとの間の非接触通信での認証時に、前回の端末設定の結果を取得して、前回機器1と機器2との間で有効にした設定が正しく無効化されている場合のみ、今回の機器2であるコンビカード20と機器3であるゲートとの間の認証を許可するようにしても勿論よい。

[0168] 次に図を参照して動作を説明する。

[0169] 図36は、第8の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス図である。

[0170] まず、端末アプリおよびそのデータの退避時の処理から説明すると、本実施形態の場合、機器2であるコンビカード20の非接触通信手段(3)22が、機器3であるゲート40の非接触通信手段(4)41と非接触通信を行い、機器3であるゲート40のゲートアプリ43から機器2であるコンビカード20の認証アプリ24に対し、認証要求が送信された場合(9－1)、コンビカード20のCPU23は、機器3であるゲート40との間で認証処理を行う(9－2)。

[0171] そして、認証処理がOKであった場合、コンビカード20の認証アプリ24は、前回の結果を端末設定管理部220に対し要求し(9－3)、端末設定管理部220は、前回の結果がOKであれば、認証アプリ24に対し前回結果OKを返す(9－4)。

[0172] すると、認証アプリ24は、ゲート40のゲートアプリ43に対し、前回結果OKを通知して(9－5)、ゲート40のゲートアプリ43は、ゲートをオープンにする(9－6)。なお、この機器2であるコンビカード20と機器3であるゲート40との間の非接触通信での認証時に前回の端末設定の結果を取得した際、前回有効にした設定が正しく無効化されていない場合は、認証を許可しないようにする。

[0173] また、コンビカード20の認証アプリ24は、前回結果OKと判断された場合、機器1である携帯端末10に対しインストール要求を送信する(9－7)。

[0174] すると、携帯端末10のCPU12は、端末アプリ退避管理部120に対しインストール可否を問い合わせ(9－8)、端末アプリ退避管理部120がインストールの可否を判断する(9－9)。そして、インストール可と判断した場合、端末アプリ退避管理部120は

、コンビカード20の端末設定管理部220に対し、アプリ退避要求を送信して(9－10)、端末アプリ退避管理部120と端末設定管理部220との間で認証処理を行う(9－11)。

[0175] その認証結果がOKの場合、端末アプリ退避管理部120は、携帯電話10から退避させるべき端末アプリおよびそのデータを、コンビカード20側の例えば端末設定管理部220に対し送信し(9－12)、端末設定管理部220に退避させるべき端末アプリおよびそのデータを格納させる(9－13)。

[0176] そして、その格納処理が無事終了した場合、コンビカード20の端末設定管理部220は、格納OKの結果通知を、携帯端末10の端末アプリ退避管理部120に対し送信し(9－14)、端末アプリ退避管理部120は、CPU12に対し応答可かを返信する(9－15)。

[0177] すると、携帯電話10のCPU12は、コンビカード20の認証アプリ24との間で認証処理を実行し(9－16)、その認証処理がOKの場合には、コンビカード20の認証アプリ24から携帯電話10のCPU12に対し新たにインストールする端末アプリが送信され(9－17)、送信された端末アプリを受信してインストールする(9－18)。

[0178] 携帯電話10のCPU12は、コンビカード20から受信した端末アプリ27がインストールできた場合は、インストール結果OKの通知をコンビカード20の認証アプリ24に対し行ない(9－19)、認証アプリ24は端末設定管理部220に対し設定通知を行なう(9－20)。

[0179] 端末設定管理部220は、認証アプリ24からの設定通知により、第7の実施形態と同様に、図33に示すID、機器3のID、ゲートアプリID、機器1のID、設定時のタイムスタンプ、有効時間、認証情報DBのID、インストールした時の端末アプリID、インストールした設定命令ID、削除した設定命令ID、設定処理結果を格納する(9－21)。

[0180] 端末設定管理部220は、かかるデータの格納後、格納結果OKの通知を認証アプリ24に対し行う(9－22)。これで、携帯電話10において先に保存されている端末アプリをコンビカード20へ退避しての新たな端末アプリのインストール時の処理が終了する。なお、第7の実施形態と同様に、コンビカード20では、端末設定管理部220は、認証アプリ24またはCPU23と一体でも勿論よい。

[0181] 次に、復活時の処理について説明する。

[0182] 復活時の処理は、機器1である携帯端末10のCPU12が、まず、タイマー管理によりインストールした端末アプリの削除処理を行い(9－23)、その削除処理が終了した場合、端末アプリ退避管理部120に対し、復活要または不要の問い合わせを行う(9－24)。

[0183] 端末アプリ退避管理部120は、その問い合わせを受けて、復活要または不要の判断を行い(9－25)、端末アプリを退避させており復活をする必要がある場合は、コンビカード20の端末設定管理部220に対し復活要急を送信し(9－26)、端末アプリ退避管理部120と端末設定管理部220との間で認証処理を行う(9－27)。

[0184] その認証処理の結果、認証がOKの場合は、端末設定管理部220は端末アプリ退避管理部120に対し退避させていた端末アプリおよびその端末データのデータを送信し(9－28)、端末アプリ退避管理部120はその退避させていた端末アプリおよびその端末データのデータを受信してメモリ等にインストールして復活し(9－29)、復活結果を端末設定管理部220に対し送信する(9－30)。

[0185] すると、端末設定管理部220は、端末アプリ退避管理部120からの復活結果を、例えば、図33に示す認証情報等に格納し(9－31)、格納結果OKであれば、その格納結果OKを端末アプリ退避管理部120へ通知する(9－32)。端末アプリ退避管理部120は、CPU12に対し復活完了通知を行い(9－33)、復活時の処理が終了する。

[0186] なお、端末アプリ退避管理部120と端末設定管理部220との間の認証処理(9－11)は、端末アプリ退避管理部120から端末設定管理部220へのアプリ退避要求(9－10)の前でもよく、携帯電話10のCPU12と、コンビカード20の認証アプリ24との間の認証処理(9－16)は、認証アプリ24から携帯電話10のCPU12へのインストール要求(9－7)の前でもよい。また、復活時の処理における端末アプリ管理部120と認証アプリ24との間における認証処理は、CPU12から復活要または不要の問い合わせを受ける(9－24)前に実行しても良い。さらに、機器2であるコンビカード20を機器1である携帯電話10に装着した時点で認証する形態をとる場合には、端末アプリ退避管理部120と端末設定管理部220との間の認証処理(9－11, 9－27)や、携

帯電話10のCPU12と認証アプリ24との間の認証処理(9－16)などは、不要となり、省略しても良い。

[0187] また、機器2であるコンビカード20にタイマー機能がある場合には、コンビカード20で時間管理を行い、設定時間になると、機器1のCPU12によるタイマー管理による削除処理(9－23)の前に、機器2から機器1にタイマー機能に基づき削除命令を送って、機器1ではこの削除命令により削除処理を行うようにしてもよい。この場合、機器2の端末設定管理部220と、機器1の端末アプリ退避管理部120との間の認証処理(9－25)は、機器2から機器1への削除命令の前に、または機器1のCPU12によるタイマー管理による削除処理(9－23)の前に行ってもよい。

[0188] 図37に、第8の実施形態の端末アプリ退避管理部120における詳細処理を示すフローチャートである。

[0189] 端末アプリ退避管理部120では、まず、CPU12からの端末アプリのインストール可否の問い合わせか否かを判断し(ステップ1000)、インストール可の場合は(ステップ1000"YES")、アプリ管理テーブル(図示せず)等を確認して(ステップ1100)、端末アプリを退避させずインストールできるか否かを判断する(ステップ1200)。

[0190] 例えば、アプリ管理テーブル(図示せず)等を確認して、格納可能な端末アプリの最大個数が10コで、すでに端末アプリが10コ格納されている場合には、端末アプリを退避させずの新規インストールはできないと判断する。なお、インストール可否問い合わせとしては、例えば、可否問合せID1として、アプリID3の端末アプリを削除し、アプリID1，アプリID2の端末アプリを2つインストールしたいという例が考えられる。

[0191] そして、端末アプリを退避させずインストール可能と判断した場合(ステップ1200"YES")、端末アプリ退避管理部120は、CPU12にインストール可能を通知して、端末アプリを退避させずインストールを実行させる(ステップ1250)。

[0192] 一方、端末アプリを退避させずインストール不可と判断した場合(ステップ1200"NO")、端末アプリ退避管理部120は、まず、機器2であるコンビカード20に退避させる端末アプリを決定する(ステップ1300)。例えば、端末アプリの退避優先度テーブル(図示せず)等を参照して、アプリID8のゲームの端末アプリ等を退避することに決定する。

[0193] 端末アプリ退避管理部120は、退避させる端末アプリを決定すると、機器2の端末設定管理部220に対し、退避要求を送信し、アプリ退避処理を実施し(ステップ1400)、その退避結果を管理テーブル等に格納して(ステップ1500)、スタートに戻る。例えば、アプリID8のゲームの端末アプリの退避処理を行った場合、その端末アプリの可否問合せID1や、退避時のタイムスタンプ、退避結果OK、退避したアプリID(アプリID8)、機器2との認証情報等を、管理テーブル等に格納する。

[0194] 一方、ステップ3700にて、インストール可否の問い合わせではなく(ステップ1000"NO")、復活要否の問い合わせであると判断した場合(ステップ1600"YES")、復活処理が必要か否かを、アプリ管理テーブル(図示せず)等を参照して確認する(ステップ1700)。

[0195] 復活要否の問い合わせとしては、例えば、インストール可否問合せの可否問合ID1の設定を解除したので、復活処理が必要であれば復活処理を実行する等の復活要否問合せID2が考えられる。また、復活処理が必要か否かをアプリ管理テーブル(図示せず)等を参照して確認した際に、可否問合せID1ではアプリID8のゲームの端末アプリの退避処理を実施、等と記載されている場合は、復活処理が必要と判断する。

[0196] ここで、復活が不要と判断した場合には(ステップ1800"NO")、CPU12に完了を通知して(ステップ1850)、スタートに戻る一方、復活が必要と判断した場合には(ステップ1800"YES")、端末アプリ退避管理部120は、機器2の端末設定管理部220に対し復活要求を送信し、機器2の端末設定管理部220等に退避させておいた端末アプリの復活処理を実施する(ステップ1900)。そして、復活処理の結果をアプリ管理テーブル(図示せず)等に格納して、CPU12にその結果を通知し(ステップ1950)、最初に戻る。復活処理の結果としては、例えば、可否問合せID1、退避時のタイムスタンプ、退避結果OK、要否問合せID2、復活時のタイムスタンプ、復活結果OK、退避・復活したアプリID(アプリID8)、機器2との認証情報等がある。

[0197] このように、第8の実施形態によれば、機器1である携帯電話10に新たな端末アプリをインストールする場合、携帯電話10のメモリ容量確保等のため、携帯電話10の端末アプリをコンビカード20に退避させて、新たな端末アプリを携帯電話10にインス

トールし、タイマーの管理等により新たにインストールした端末アプリの設定解除を行った場合には、退避させておいた端末アプリを携帯電話にインストールするようにしたため、携帯電話10のメモリ容量をそれほど増やさずに、カードアプリ機能や装置機能等が発現されるエリアを限定することができる。

[0198] 以上説明したように、本発明の一態様では、セキュアデバイスに、ゲート機器に対して認証処理を行う認証手段と、端末にインストールする端末アプリと、認証手段がゲート機器との認証に成功した場合に、ゲート機器から指定された端末アプリを端末にインストールする制御手段とを設けているため、セキュアデバイスをゲート機器に翳し、正常に通過したエリアでのみ、端末アプリが端末にインストールされる。ゲート機器のゲートアプリが特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末へのGPS受信機等の装備も必要がない。

[0199] また、本発明の別の態様では、セキュアデバイスに、ゲート機器に対して認証処理を行う認証手段と、カードアプリとを設け、認証手段がゲート機器との認証に成功した場合に、ゲート機器から指定されたカードアプリが、端末の端末アプリのアクセスを許容するようにしたため、セキュアデバイスをゲート機器に翳し、正常に通過したエリアでのみ、端末アプリは、カードアプリの利用が可能になる。

[0200] また、本発明の別の態様では、セキュアデバイスに、ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する認証手段と、認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対して、この機器の検証に供するためにゲート機器の識別情報を送信し、または、この機器に代わって識別情報を検証するカードアプリとを設けたため、ゲート機器が設置された正規の入口から入場しないと、機器は動作しないようにすることができる。

[0201] また、本発明の別の態様では、セキュアデバイスは、ゲート機器との間の通信方式に応じて、端末にインストールあるいは端末から削除する端末アプリケーションを設定するようにしたため、通信方式に応じて簡単に端末にインストールする端末アプリケーション等を変更することができ、セキュリティを簡単に確保することができる。

[0202] また、本発明の別の態様では、セキュアデバイスは、ゲート機器との間で認証を行なう際、端末との間で前回有効にした設定が正しく無効化されているか否かを判断し

、正しく無効化されている場合のみ、ゲート機器との間の認証を許可するようにしたため、前回の無効化処理が正しく行われたか否かに基づいて今回のゲート機器との認証を許可することができ、よりセキュリティを確保することができる。

[0203] また、本発明の別の態様では、セキュアデバイスは、ゲート機器との間の通信方式に応じて、カードアプリケーションの有効または無効を設定するようにしたため、通信方式に応じて簡単にセキュリティを確保することができる。

[0204] また、本発明の別の態様では、ゲート機器に、セキュアデバイスまたはセキュアデバイスを保持する端末との通信手段と、通信手段を通じてセキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリを指定するゲートアプリとを設けたり、あるいは、ゲート機器に、セキュアデバイスまたはセキュアデバイスを保持する端末との通信手段と、通信手段を通じてセキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末の端末アプリがアクセスできるカードアプリを指定するゲートアプリとを設けるようにしたため、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリや、端末アプリがアクセス可能となるカードアプリを指定することができる。

[0205] また、本発明の別の態様では、端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功したセキュアデバイスから、ゲート機器が指定した端末アプリをインストールするようにしたり、あるいは、端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功したセキュアデバイスが保持するカードアプリの中で、ゲート機器が指定したカードアプリにアクセスする端末アプリを備えるようにしたため、入口にゲート機器が設置された特定のエリアの中でのみ、端末装置の特殊な機能が発揮できる。

[0206] また、本発明の別の態様では、端末装置は、セキュアデバイスからの新たな端末アプリケーションのインストール要求受信時に、メモリ容量が少なく前記新たな端末アプリケーションをインストールできない場合には、保持している端末アプリケーションを前記セキュアデバイスに退避させてから前記新たな端末アプリケーションをインストールし、その後、インストールした前記新たな端末アプリケーションを削除して、前記退避させた端末アプリケーションを復活させるようにしたため、端末アプリケーションを保存

するためのメモリ容量が少ない場合でも、新たな端末アプリケーションを実施させることができる。

[0207] また、本発明の別の態様では、機器が、ゲート機器との認証に成功したセキュアデバイスからゲート機器の識別情報を取得し、この識別情報の検証に成功した場合に所定の動作を行うようにしたり、あるいは、機器が、ゲート機器との認証に成功したセキュアデバイスからゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行うようにしたため、ユーザがセキュアデバイスを所持して正規の入口から入場しないと、機器が動作しないようにすることができる。

[0208] 本明細書は、2004年1月28日出願の特願2004－19461に基づく。この内容はすべてここに含めておく。

産業上の利用可能性

[0209] 本発明は、各種のセキュアデバイスの機能や、各種の端末、装置、機器等の機能を場所、経路、位置、または通信方式、前回の無効化処理、さらにはメモリ容量等との関連で変える場合に利用することができ、オフィス、家庭、医療現場、教育現場など、あらゆる分野での利用が可能である。

請求の範囲

[1] ゲート機器に対して認証処理を行う認証手段と、

端末にインストールする端末アプリケーションと、

前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定された端末アプリケーションを端末にインストールする制御手段と、

を備えるセキュアデバイス。

[2] ゲート機器と端末アプリケーションとの対応関係が規定された対応情報を保持し、前記制御手段は、ゲート機器から指定された端末アプリケーションと前記ゲート機器との関係が前記対応情報に合致する場合にのみ、前記端末アプリケーションを端末にインストールする請求項1に記載のセキュアデバイス。

[3] 前記制御手段は、ゲート機器との間の通信方式に応じて、前記端末にインストールあるいは前記端末から削除する端末アプリケーションを設定する請求項1に記載のセキュアデバイス。

[4] さらに、前記認証手段がゲート機器との間で認証を行なう際、端末との間で前回有効にした設定が正しく無効化されているか否かを判断し、正しく無効化されている場合のみ、前記ゲート機器との間の認証を許可する端末設定管理部を有する請求項1記載のセキュアデバイス。

[5] ゲート機器に対して認証処理を行う認証手段と、

カードアプリケーションと、

前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定されたカードアプリケーションが、端末の端末アプリケーションのアクセスを許容する制御手段と、

を備えるセキュアデバイス。

[6] 前記認証手段が認証に成功したゲート機器と前記ゲート機器から指定されたカードアプリケーションとの関係を記録するデータベースを保持し、カードアプリケーションは、端末アプリケーションからアクセス要求が有ったときに、前記データベースの情報に基づいて、アクセスの諾否を決定する請求項5に記載のセキュアデバイス。

[7] 前記制御手段は、ゲート機器との間の通信方式に応じて、前記カードアプリケーシ

ョンの有効または無効を設定する請求項5に記載のセキュアデバイス。

[8] ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する認証手段と、

前記認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対して、前記機器の検証に供するためにゲート機器の前記識別情報を送信し、または、前記機器に代わって前記識別情報を検証するカードアプリケーションと、

を備えるセキュアデバイス。

[9] 前記カードアプリケーションは、前記機器の検証に供するために、入力されたユーザ識別情報を前記機器に送信し、または、前記機器に代わって前記ユーザ識別情報を検証する請求項8に記載のセキュアデバイス。

[10] セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、

前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリケーションを指定するゲートアプリケーションと、

を備えるゲート機器。

[11] セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、

前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末の端末アプリケーションがアクセスできるカードアプリケーションを指定するゲートアプリケーションと、

を備えるゲート機器。

[12] セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスから、前記ゲート機器が指定した端末アプリケーションをインストールする端末装置。

[13] さらに、セキュアデバイスからの新たな端末アプリケーションのインストール要求受信時に、メモリ容量が少なく前記新たな端末アプリケーションをインストールできない場合には、保持している端末アプリケーションを前記セキュアデバイスに退避させてから前記新たな端末アプリケーションをインストールし、その後、インストールした前記新たな端末アプリケーションを削除して、前記退避させた端末アプリケーションを復活させる端末アプリ退避管理部、

を有する請求項12に記載の端末装置。

[14] セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスが保持するカードアプリケーションの中で、前記ゲート機器が指定したカードアプリケーションにアクセスする端末アプリケーションを備える端末装置。

[15] 前記セキュアデバイスが、着脱可能な状態で装着される請求項12に記載の端末装置。

[16] 前記セキュアデバイスが、一体的に埋め込まれる請求項12に記載の端末装置。

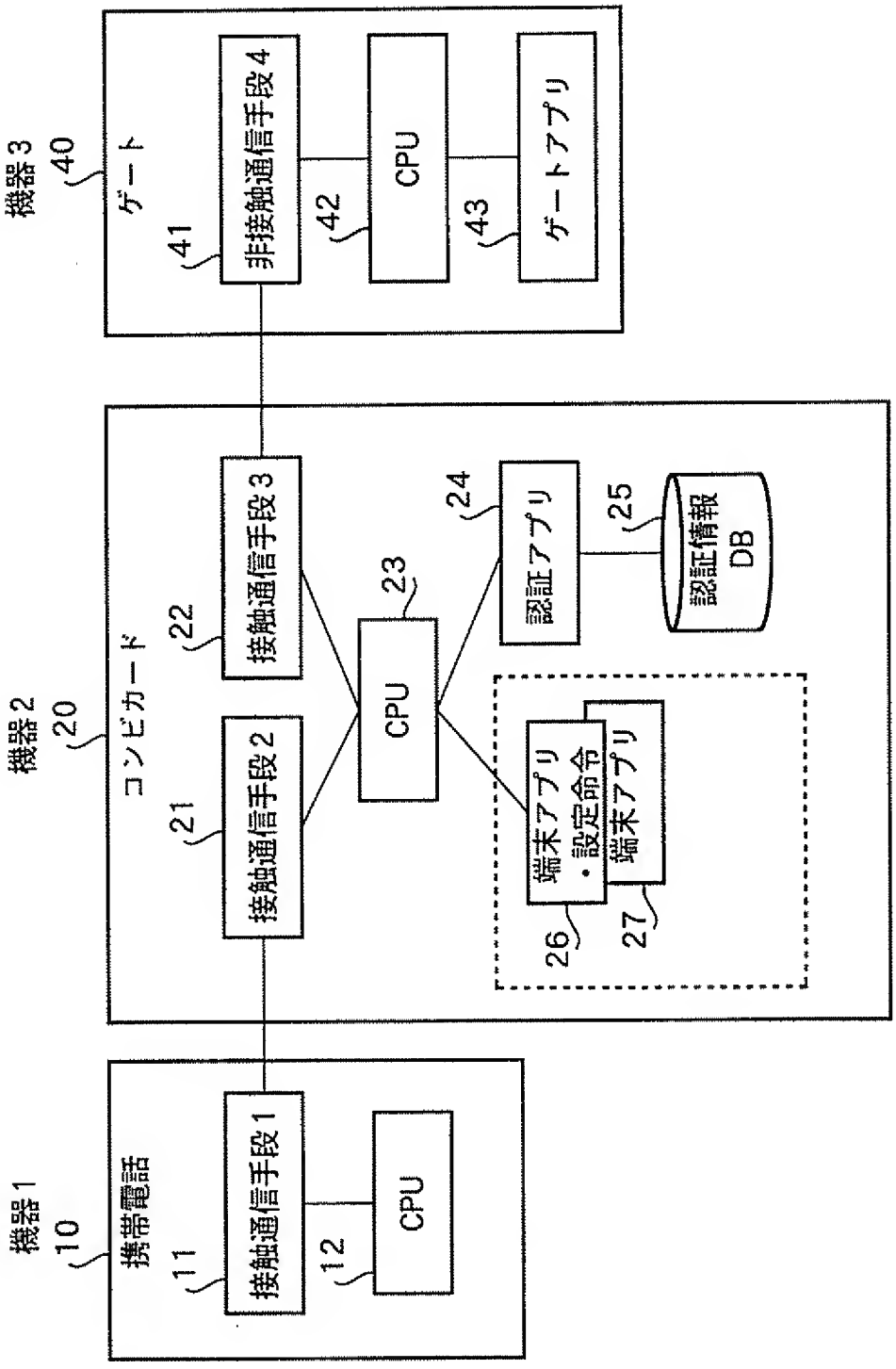
[17] ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報を取得し、前記識別情報の検証に成功した場合に所定の動作を行う機器。

[18] ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行う機器。

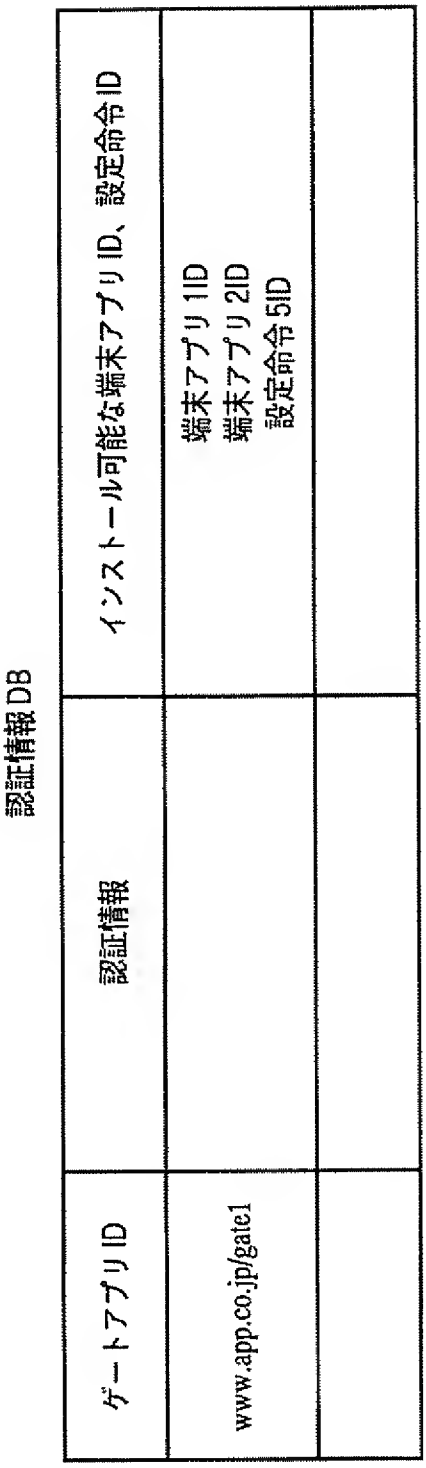
要 約 書

カードアプリ機能や装置機能等が発現されるエリアを限定できるICカード等のセキュアデバイスを提供するセキュアデバイス、端末装置、ゲート機器、機器。セキュアデバイス(20)に、ゲート機器(40)に対して認証処理を行う認証アプリ(24)と、端末である携帯電話(10)にインストールする端末アプリ・設定命令(26)や、端末アプリ(27)と、認証アプリ(24)がゲート機器(40)との認証に成功した場合に、ゲート機器(40)から指定された端末アプリを携帯電話(10)にインストールする制御手段であるCPU(23)とを設けている。セキュアデバイス(20)をゲート機器(40)に翳し、正常に通過したエリアでのみ、端末アプリ・設定命令(26)、端末アプリ(27)が携帯電話(10)にインストールされる。ゲート機器(40)のゲートアプリ(43)が特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末へのGPS受信機等の装備も必要がない。

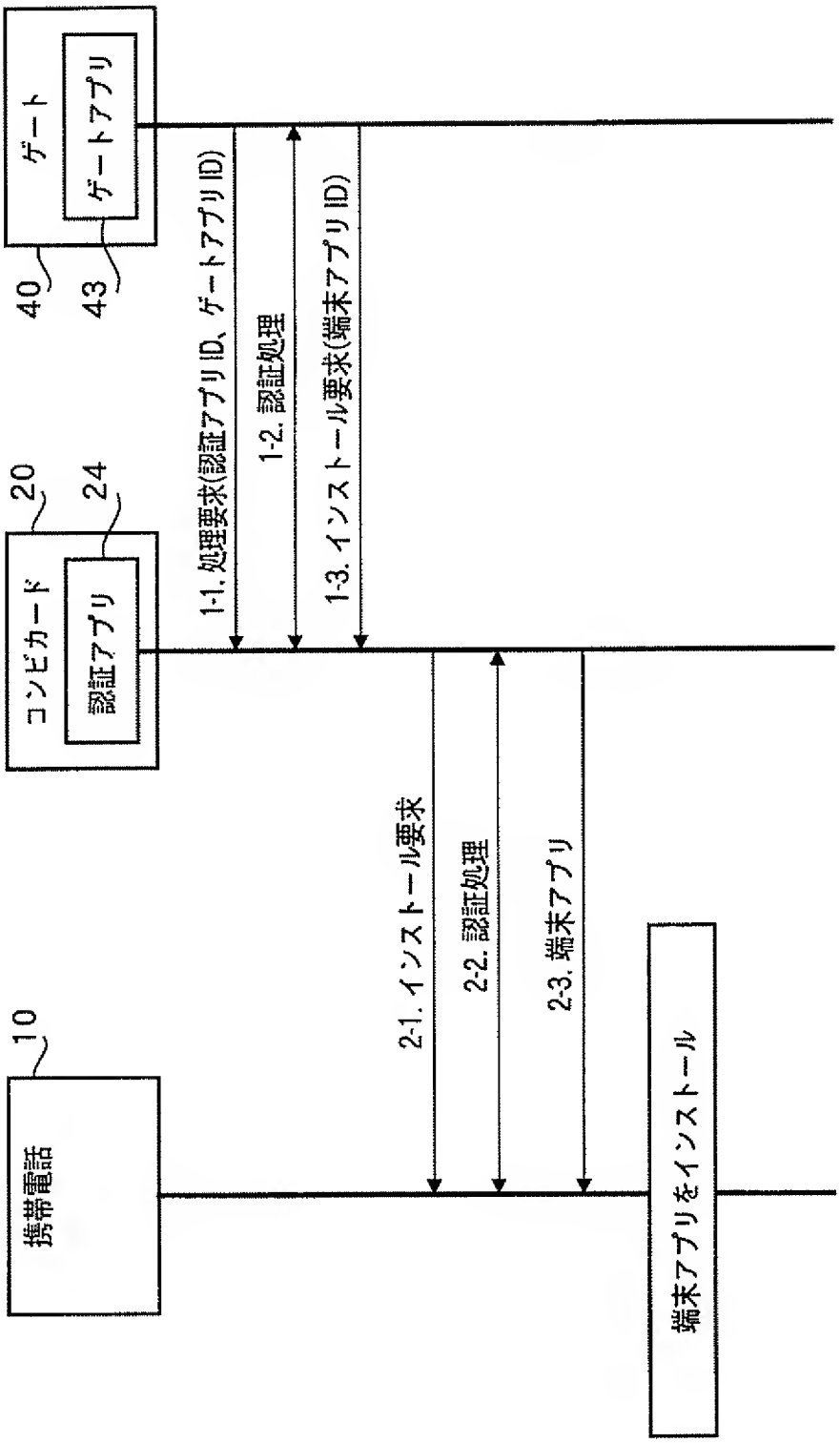
[図1]


機器1
10
携帯電話
11
接触通信手段1
12
CPU
機器2
20
コンビカード
21
接触通信手段2
22
接触通信手段3
23
CPU
24
認証アプリ
25
認証情報DB
26
端末アプリ・設定命令
27
端末アプリ
機器3
40
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ

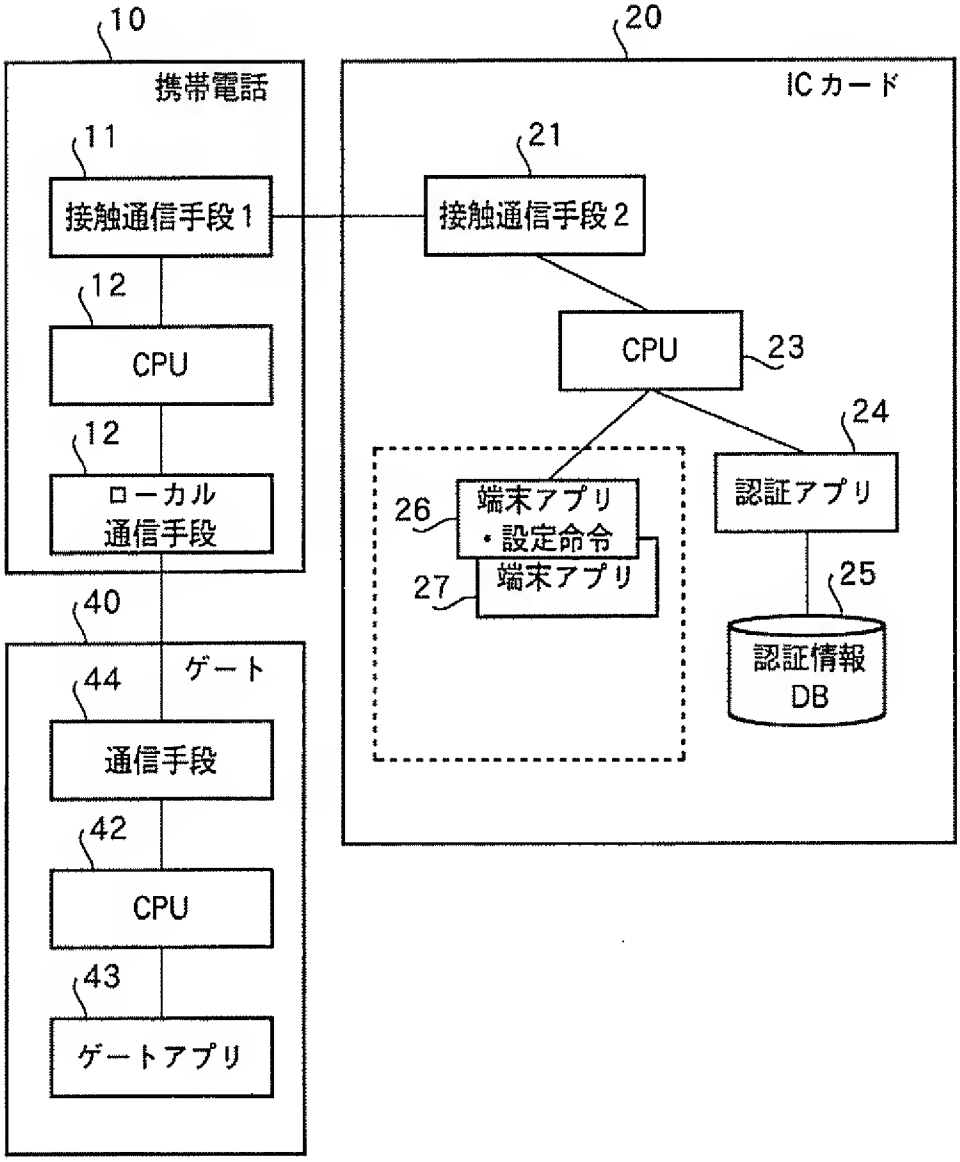
[図2]


認証情報DB
ゲートアプリID
認証情報
インストール可能な端末アプリID、設定命令ID
www.app.co.jp/gate1
端末アプリ1ID
端末アプリ2ID
設定命令5ID

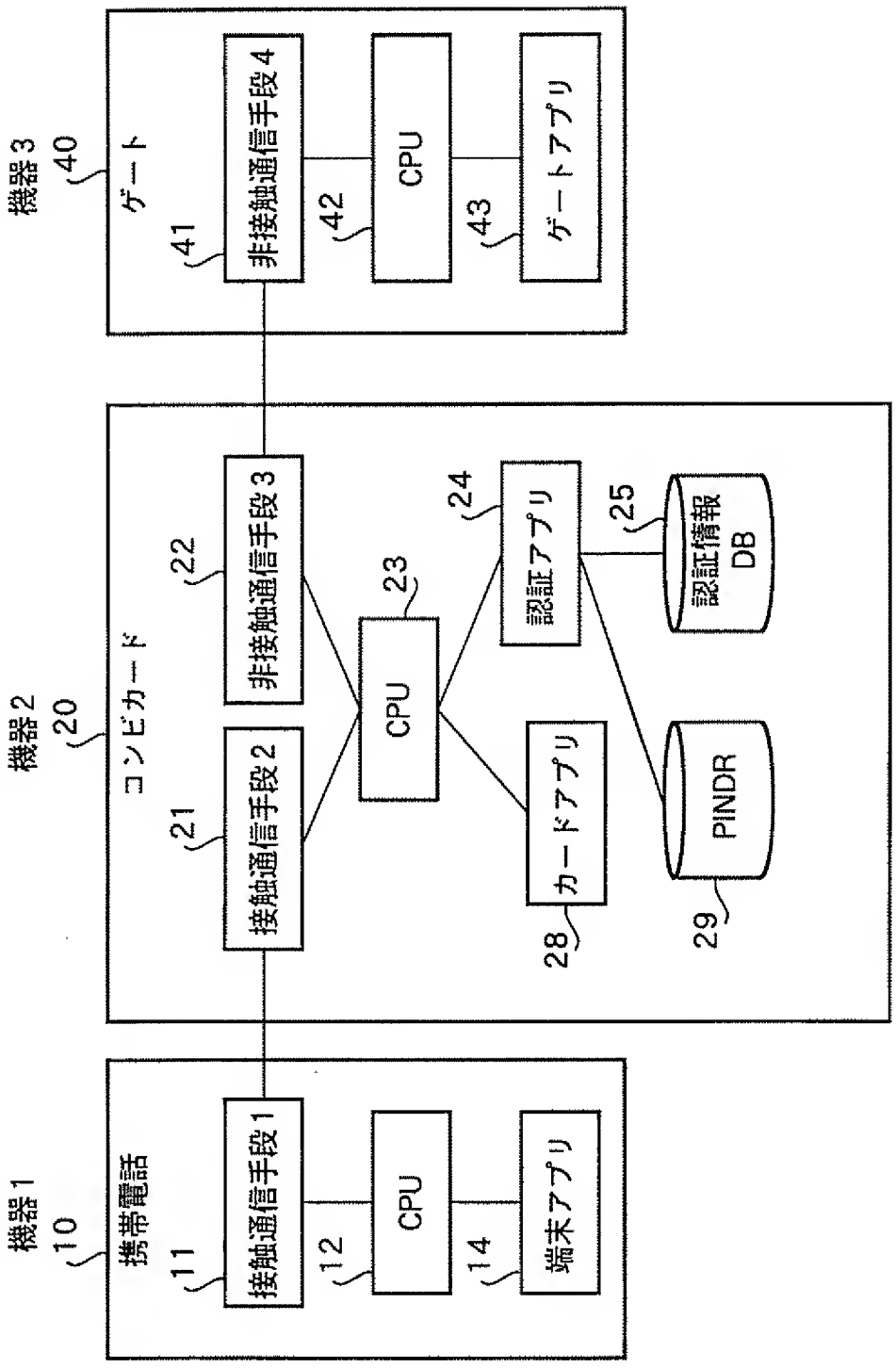
[図3]


ゲート
ゲートアプリ
40
43
コンビカード
認証アプリ
20
24
携帯電話
10
1-1. 処理要求(認証アプリID、ゲートアプリID)
1-2. 認証処理
1-3. インストール要求(端末アプリID)
2-1. インストール要求
2-2. 認証処理
2-3. 端末アプリ
端末アプリをインストール

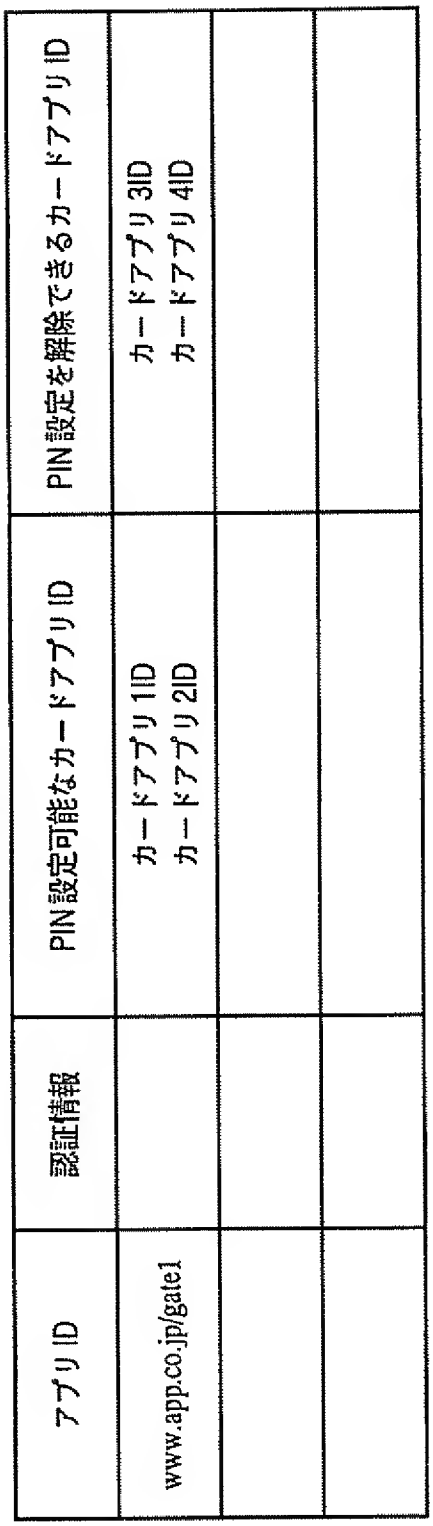
[図4]


10
携帯電話
11
接触通信手段1
12
CPU
12
ローカル
通信手段
40
ゲート
44
通信手段
42
CPU
43
ゲートアプリ
20
ICカード
21
接触通信手段2
CPU
23
24
認証アプリ
26
端末アプリ
・設定命令
27
端末アプリ
25
認証情報
DB

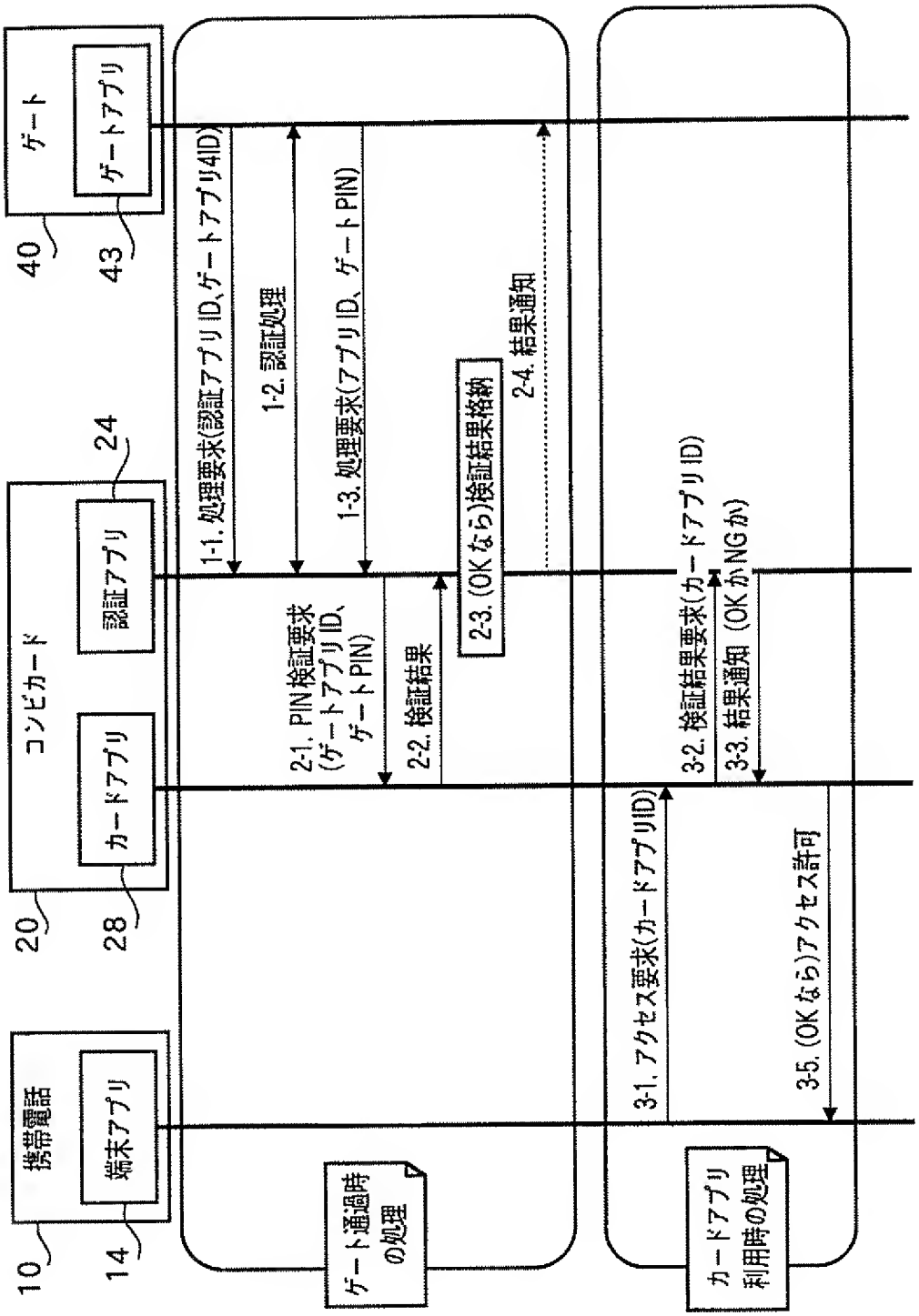
[図5]


機器1
10
携帯電話
11
接触通信手段1
12
CPU
14
端末アプリ
機器2
20
コンビカード
21
接触通信手段2
22
非接触通信手段3
23
CPU
24
認証アプリ
25
認証情報DB
28
カードアプリ
29
PINDR
機器3
40
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ

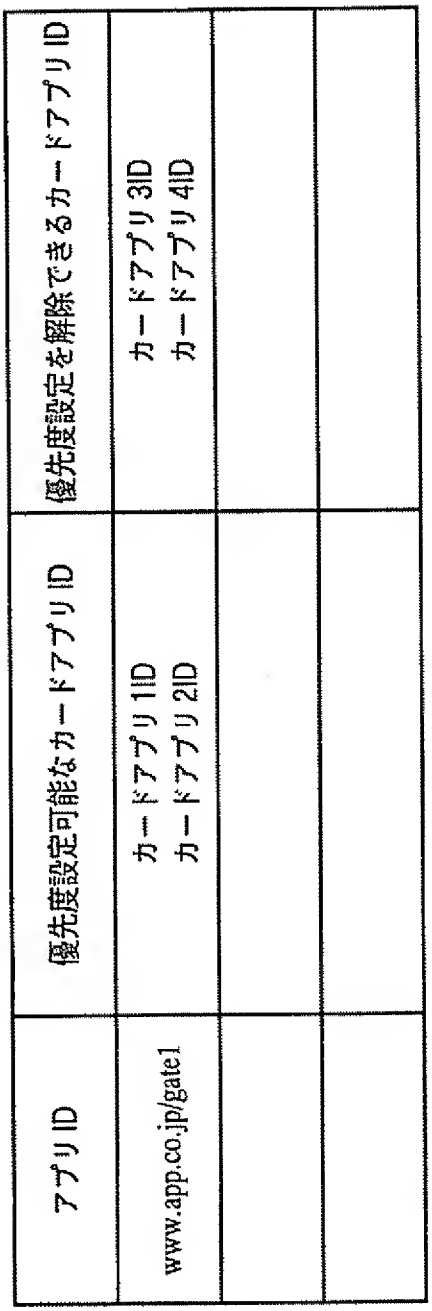
[図6]


認証情報DB
アプリID
認証情報
PIN設定可能なカードアプリID
PIN設定を解除できるカードアプリID
www.app.co.jp/gate1
カードアプリ1ID
カードアプリ2ID
カードアプリ3ID
カードアプリ4ID

[図7]

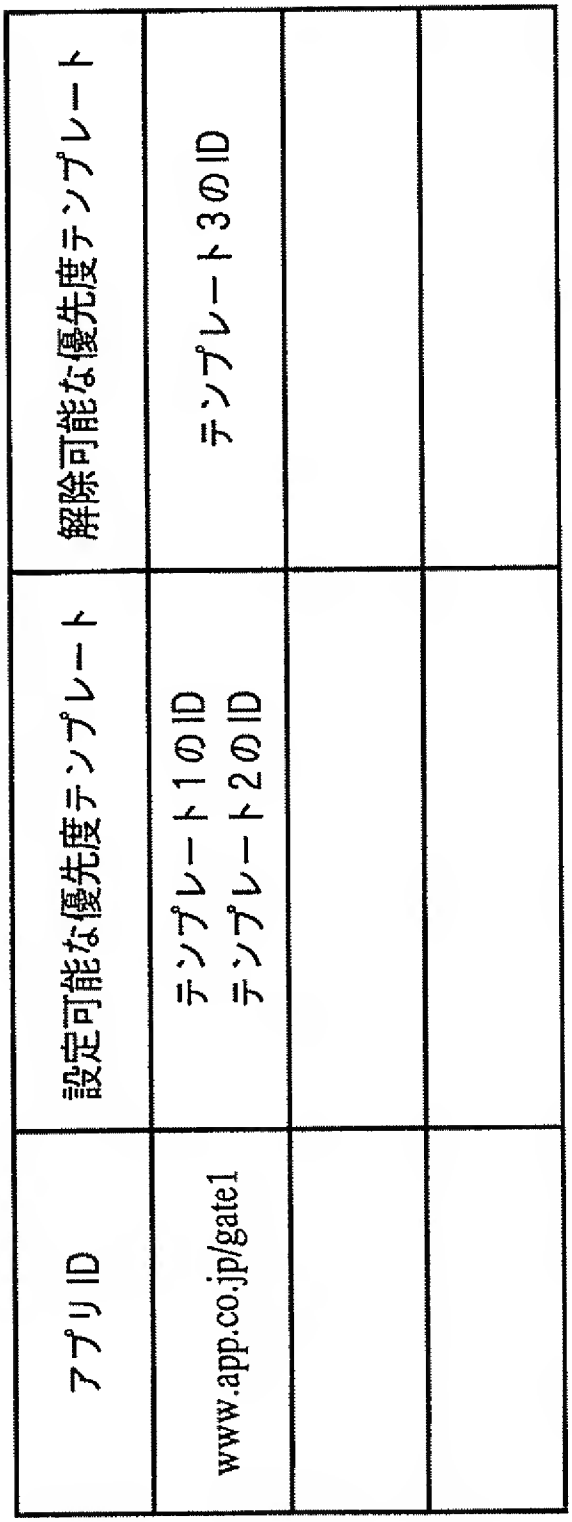

携帯電話
端末アプリ
10
14
コンビカード
カードアプリ
認証アプリ
20
28
24
ゲート
ゲートアプリ
40
43
1-1. 処理要求(認証アプリID、ゲートアプリID)
1-2. 認証処理
1-3. 処理要求(アプリID、ゲートPIN)
2-1. PIN検証要求(ゲートアプリID、ゲートPIN)
2-2. 検証結果
2-3. (OKなら)検証結果格納
2-4. 結果通知
3-1. アクセス要求(カードアプリID)
3-2. 検証結果要求(カードアプリID)
3-3. 結果通知 (OKかNGか)
3-5. (OKなら)アクセス許可
ゲート通過時の処理
カードアプリ利用時の処理

[図8]



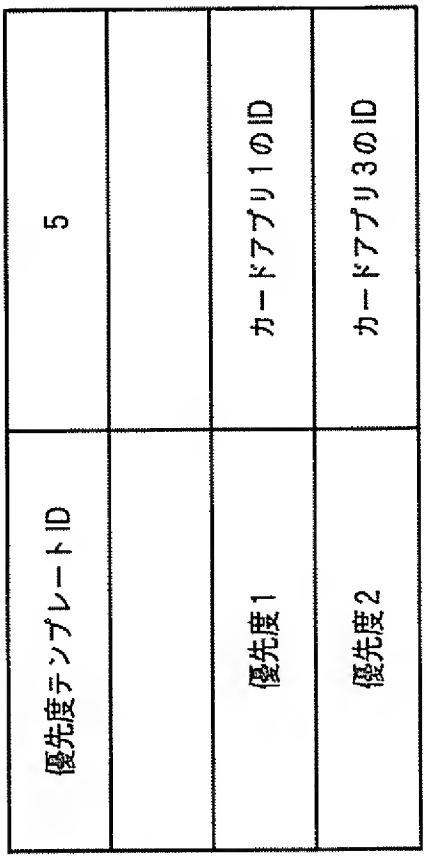
アプリID	優先度設定可能なカードアプリID	優先度設定を解除できるカードアプリID
www.app.co.jp/gate1	カードアプリ1ID カードアプリ2ID	カードアプリ3ID カードアプリ4ID

[図9A]



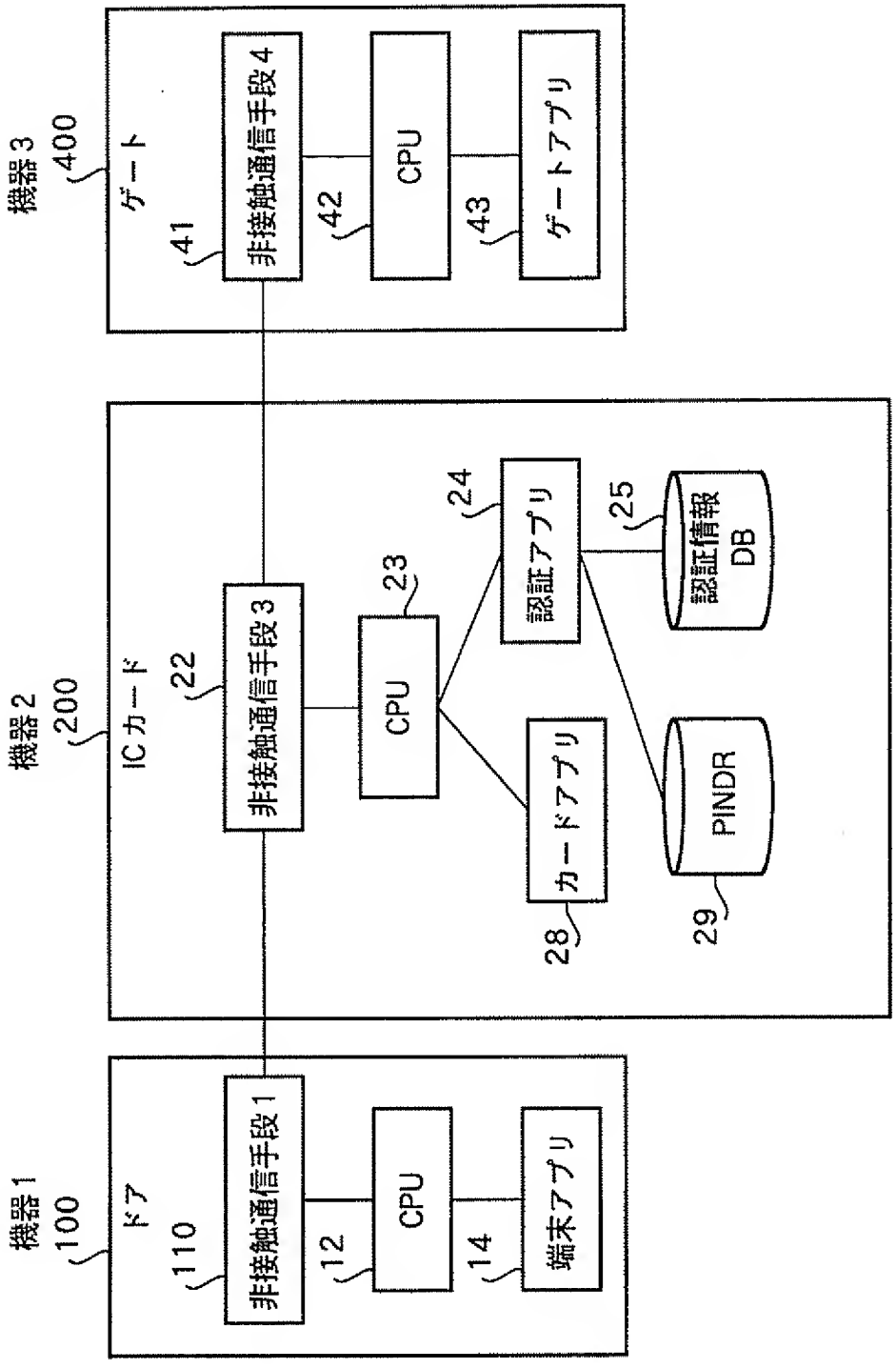
アプリID	設定可能な優先度テンプレート	解除可能な優先度テンプレート
www.app.co.jp/gate1	テンプレート1のID テンプレート2のID	テンプレート3のID

[図9B]

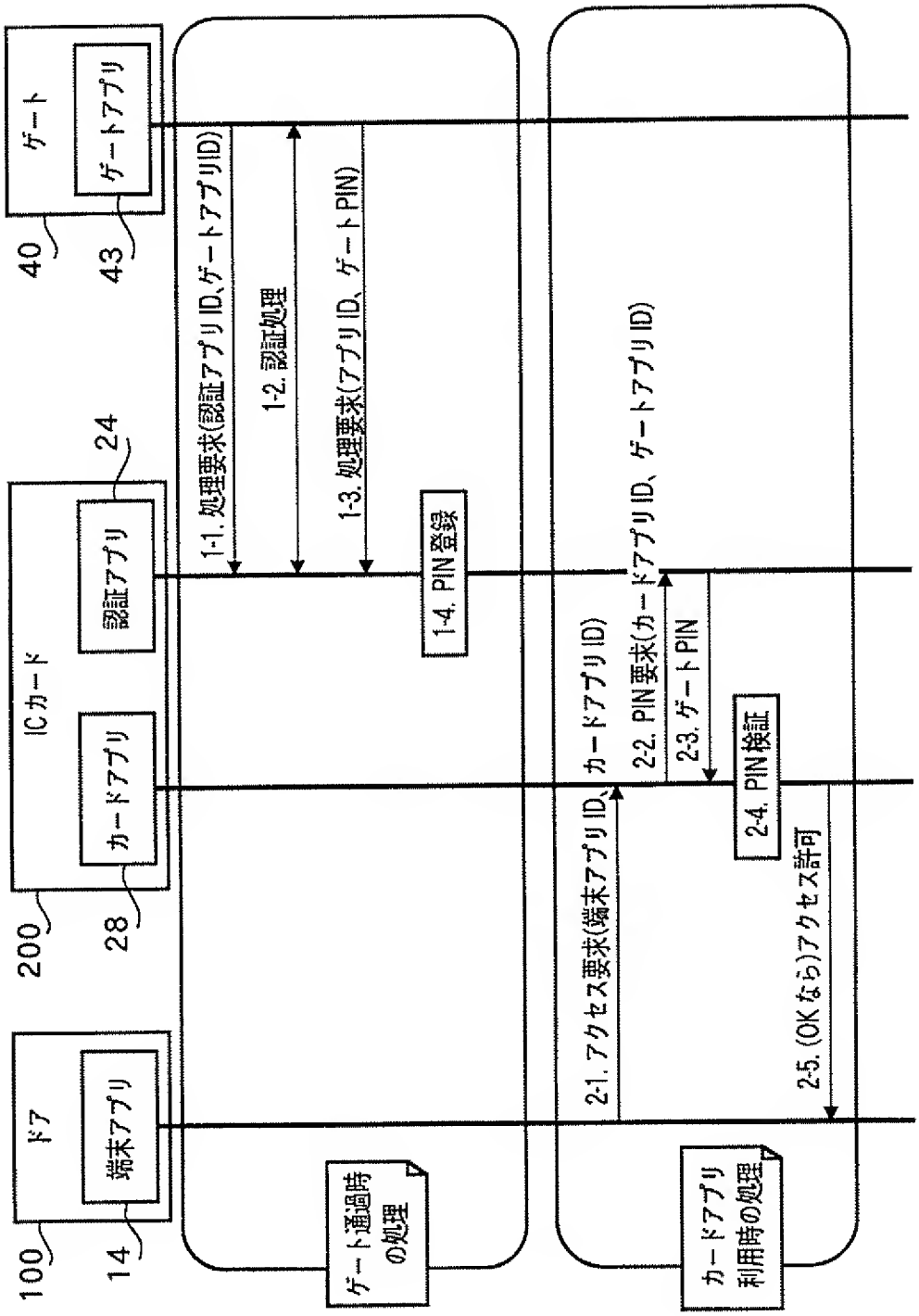


優先度テンプレートID	5
優先度1	カードアプリ1のID
優先度2	カードアプリ3のID

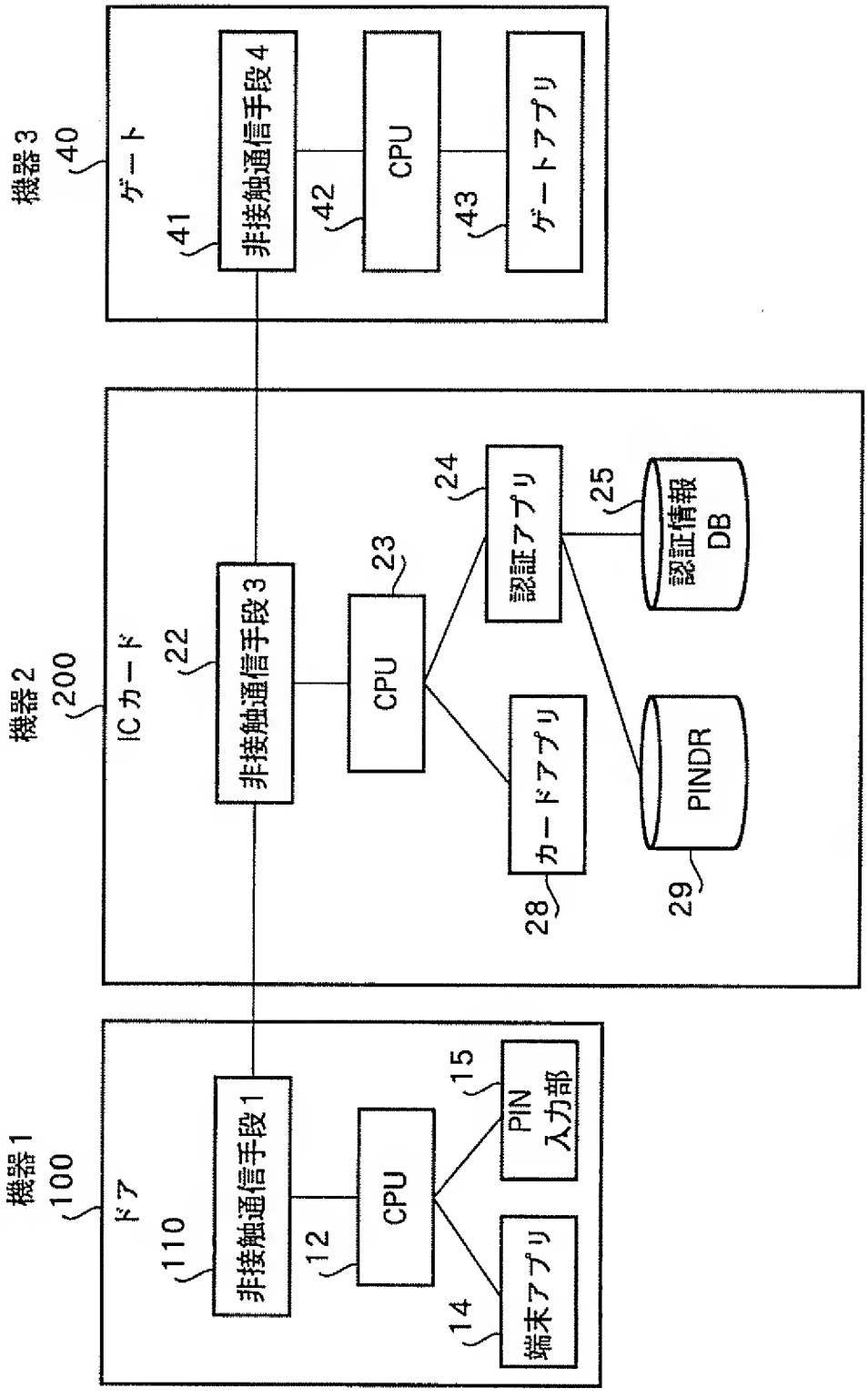
[図10]


機器1
100
ドア
110
非接触通信手段1
12
CPU
14
端末アプリ
機器2
200
ICカード
22
非接触通信手段3
23
CPU
24
認証アプリ
25
認証情報DB
カードアプリ
28
PINDR
29
機器3
400
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ

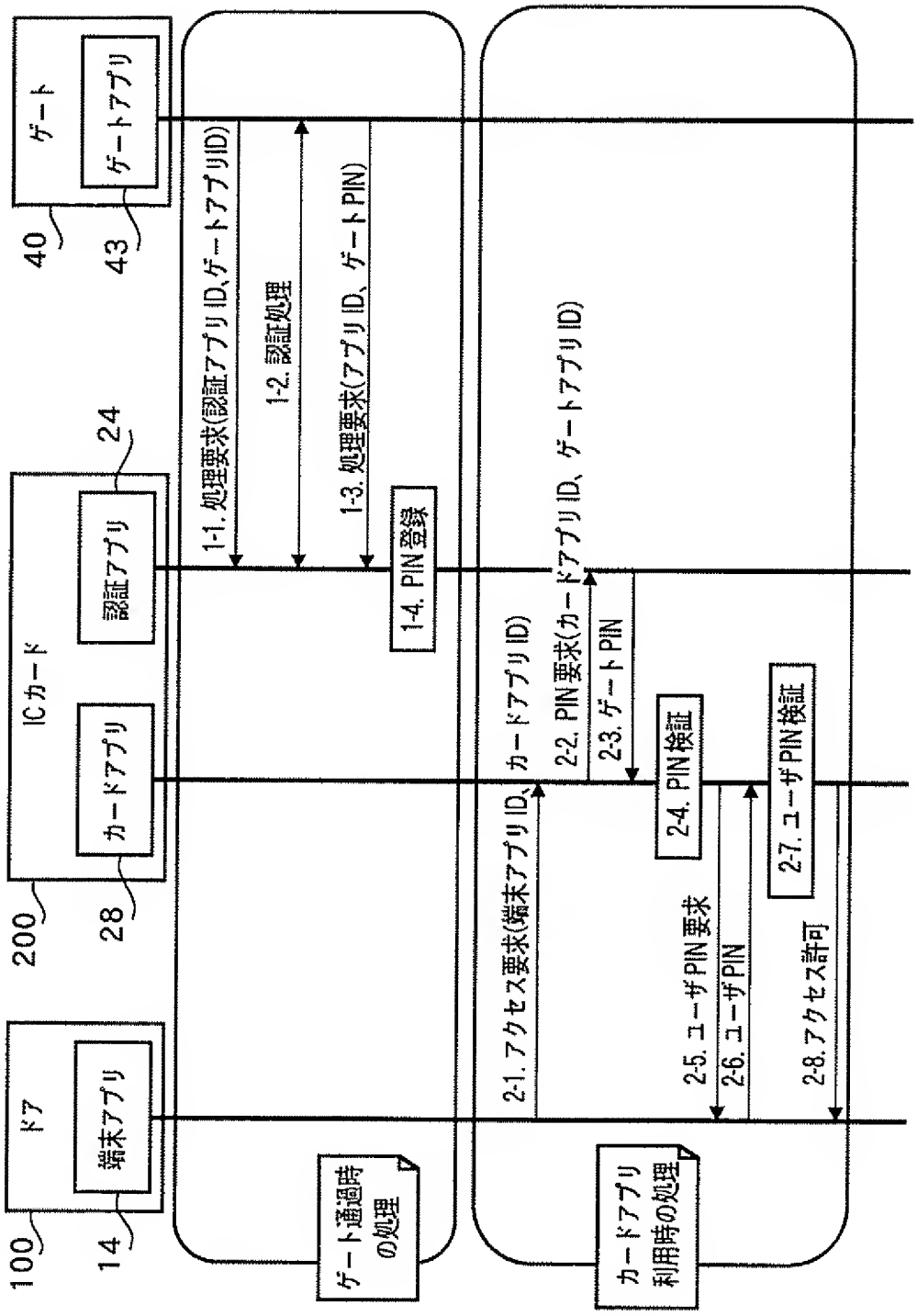
[図11]


ゲート
ゲートアプリ
40
43
ICカード
認証アプリ
カードアプリ
24
28
200
ドア
端末アプリ
100
14
1-1. 処理要求(認証アプリID,ゲートアプリID)
1-2. 認証処理
1-3. 処理要求(アプリID、ゲートPIN)
1-4. PIN登録
2-1. アクセス要求(端末アプリID、カードアプリID)
2-2. PIN要求(カードアプリID、ゲートアプリID)
2-3. ゲートPIN
2-4. PIN検証
2-5. (OKなら)アクセス許可
ゲート通過時の処理
カードアプリ利用時の処理

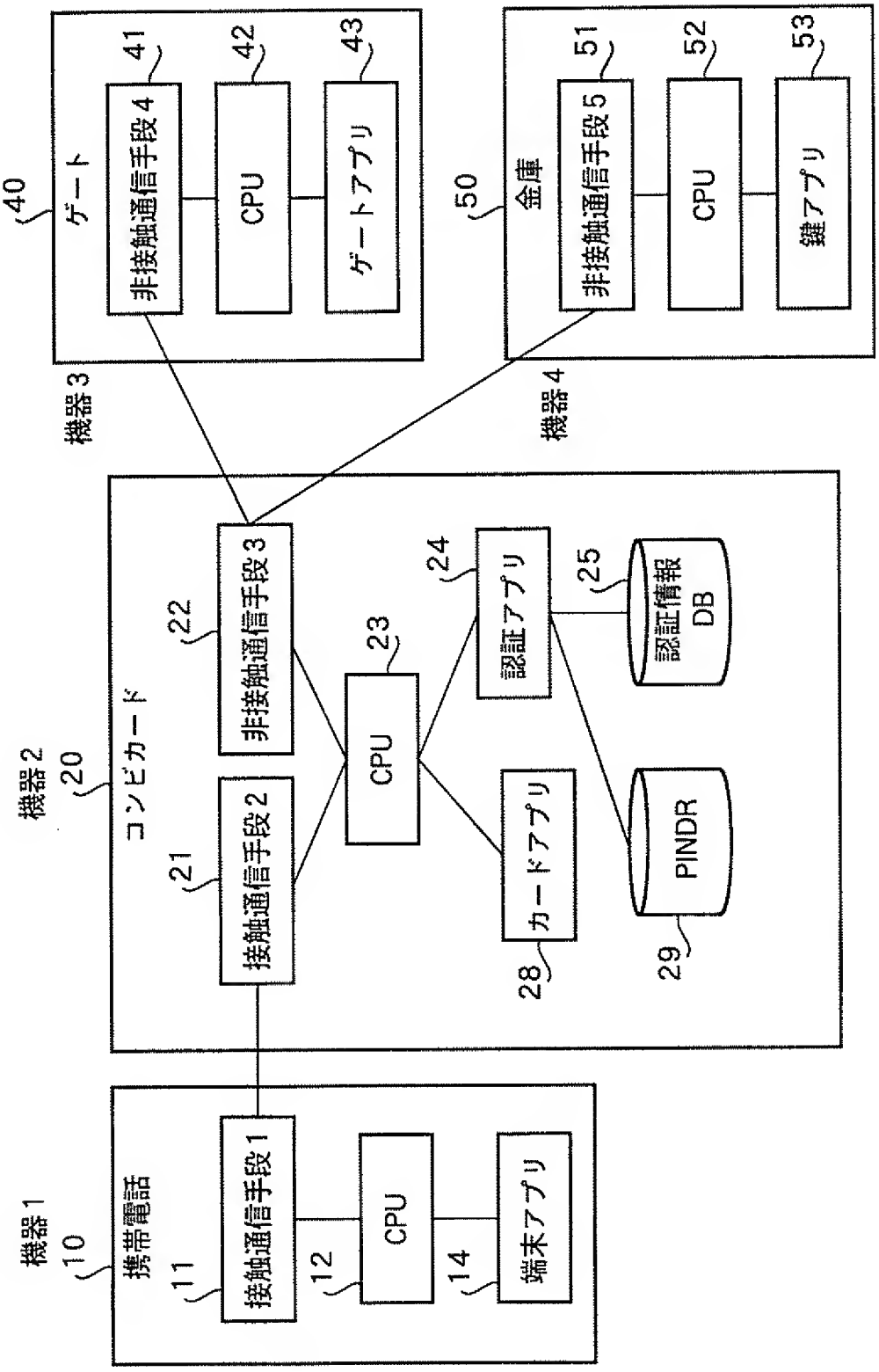
[図12]


機器1
100
ドア
110
非接触通信手段1
12
CPU
14
端末アプリ
15
PIN
入力部
機器2
200
ICカード
22
非接触通信手段3
23
CPU
24
認証アプリ
25
認証情報
DB
28
カードアプリ
29
PINDR
機器3
40
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ

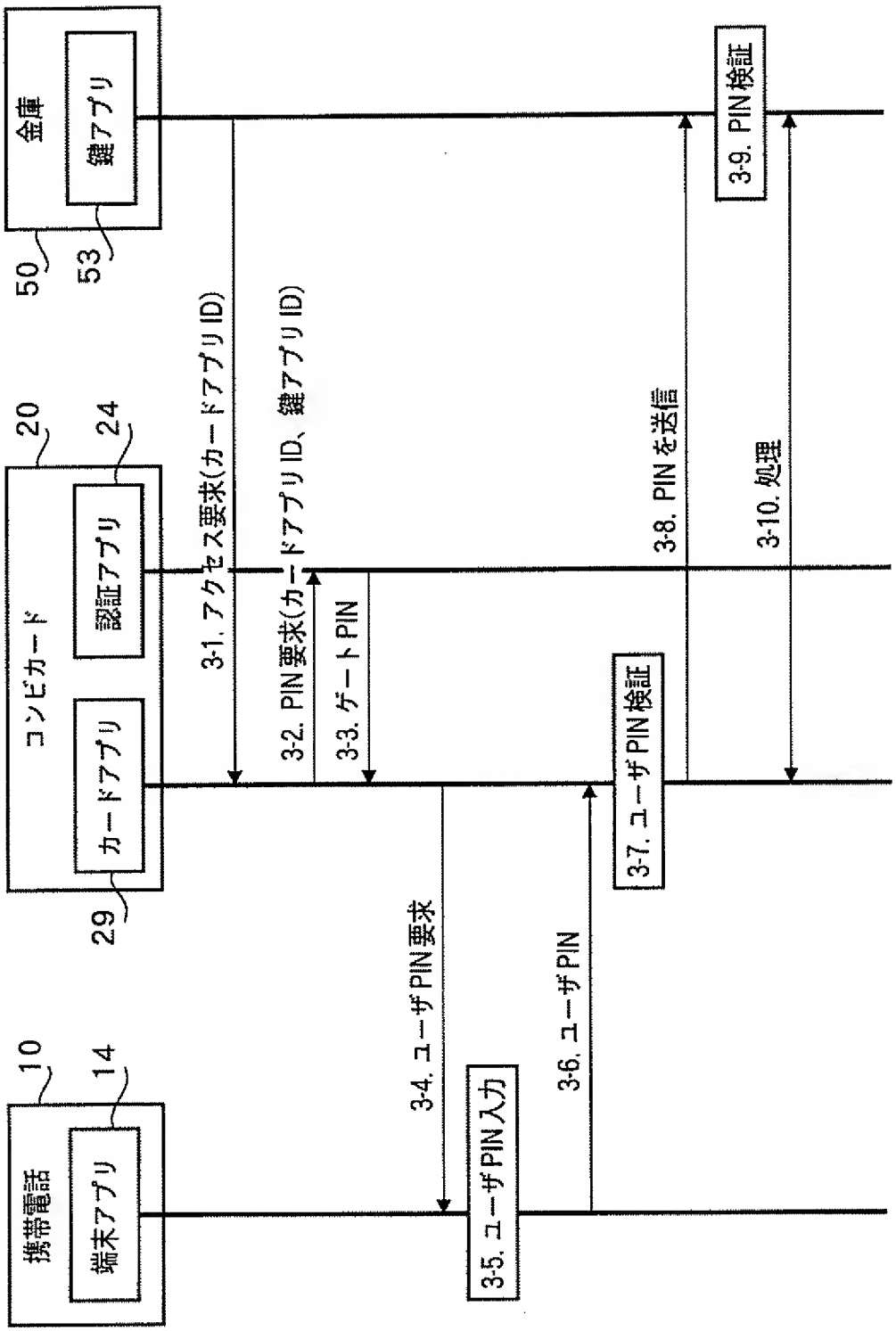
[図13]


ゲート
ゲートアプリ
40
43
ICカード
認証アプリ
24
カードアプリ
200
28
ドア
端末アプリ
100
14
1-1. 処理要求(認証アプリID,ゲートアプリID)
1-2. 認証処理
1-3. 処理要求(アプリID、ゲートPIN)
1-4. PIN登録
ゲート通過時の処理
2-1. アクセス要求(端末アプリID、カードアプリID)
2-2. PIN要求(カードアプリID、ゲートアプリID)
2-3. ゲートPIN
2-4. PIN検証
2-5. ユーザPIN要求
2-6. ユーザPIN
2-7. ユーザPIN検証
2-8. アクセス許可
カードアプリ利用時の処理

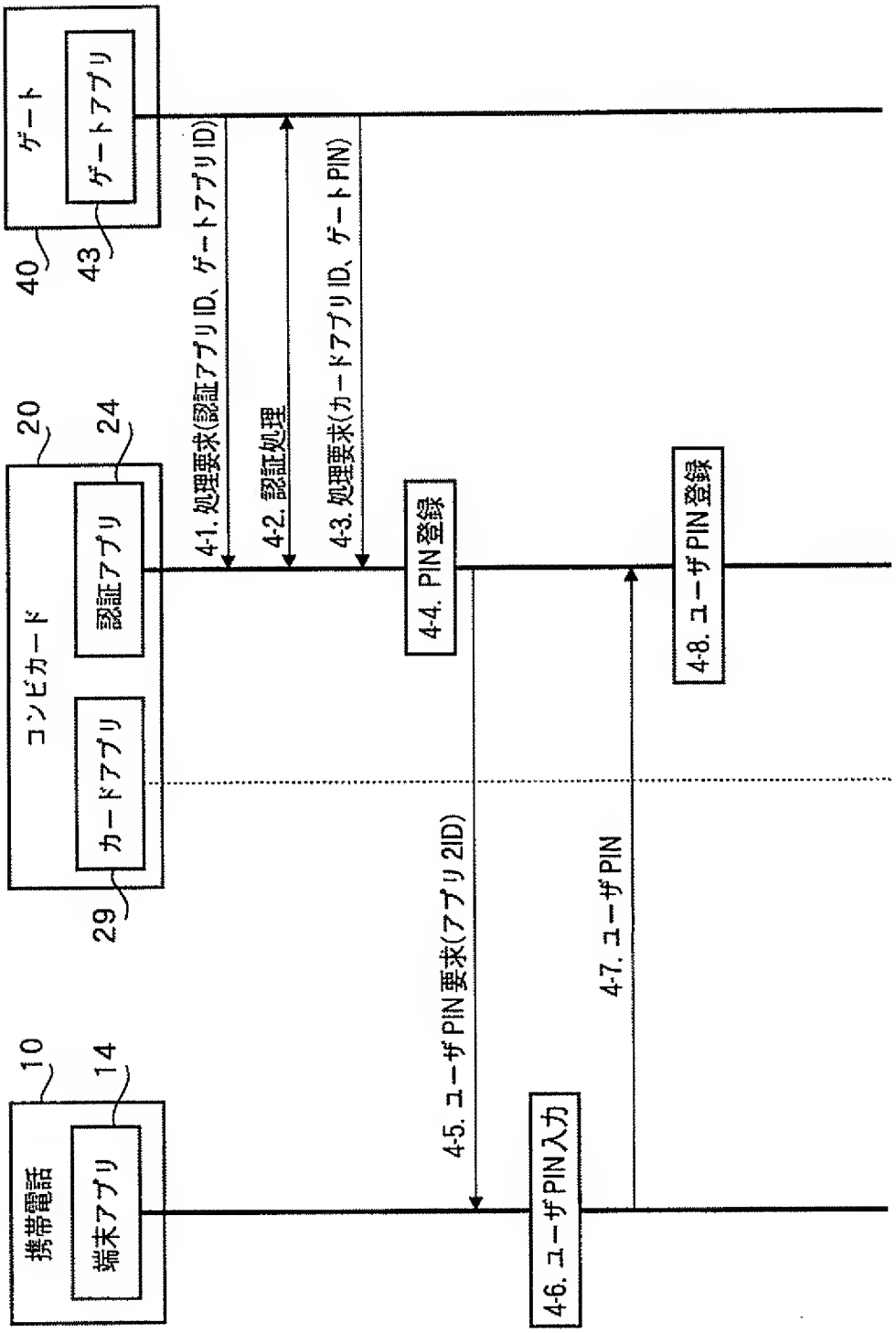
[図14]


機器1
10
携帯電話
11
接触通信手段1
12
CPU
14
端末アプリ
機器2
20
コンビカード
21
接触通信手段2
22
非接触通信手段3
23
CPU
24
認証アプリ
25
認証情報DB
28
カードアプリ
29
PINDR
機器3
40
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ
機器4
50
金庫
51
非接触通信手段5
52
CPU
53
鍵アプリ

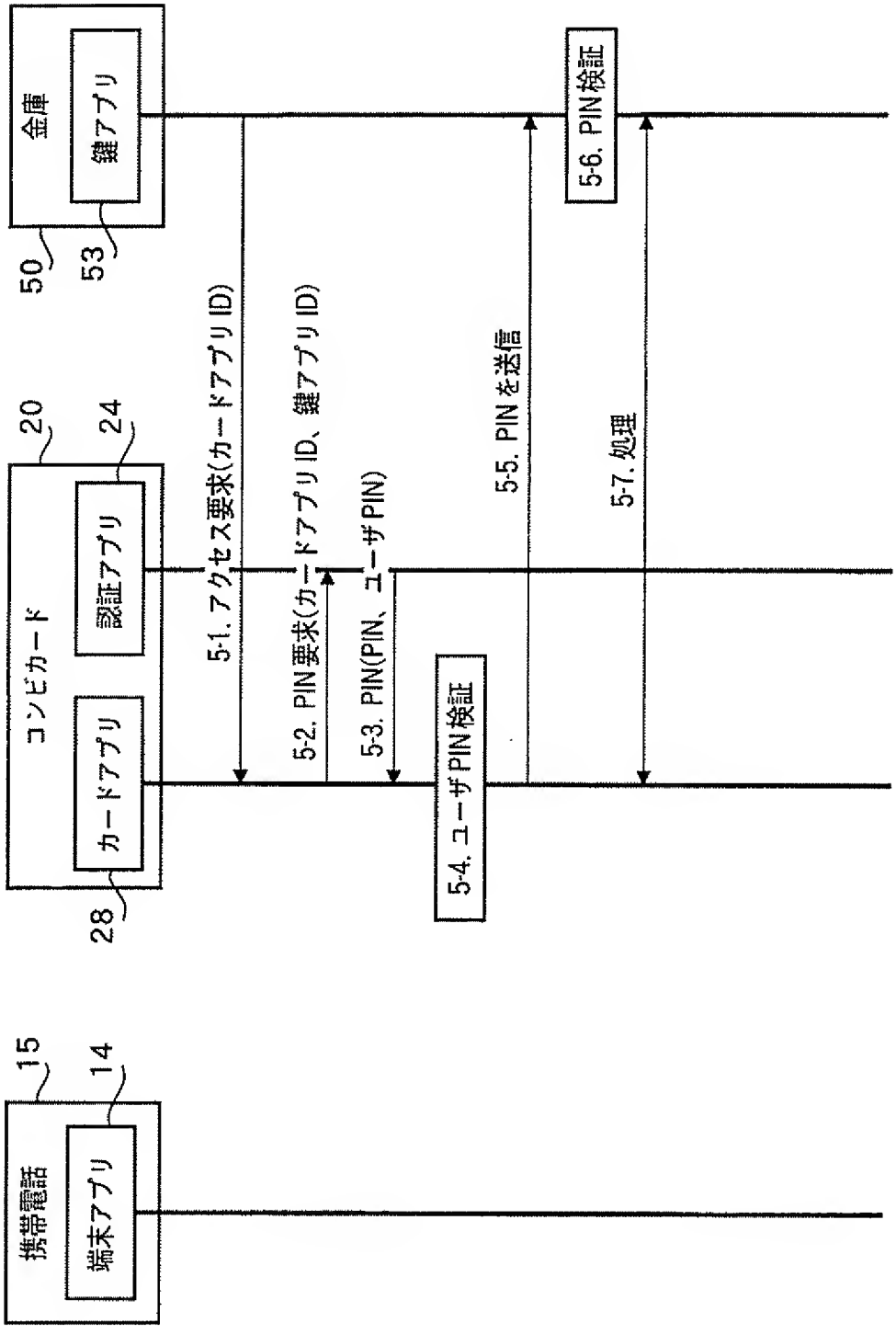
[図15]


金庫
鍵アプリ
50
53
ユンビカード
認証アプリ
カードアプリ
20
24
29
携帯電話
端末アプリ
10
14
3-1. アクセス要求(カードアプリID)
3-2. PIN要求(カードアプリID、鍵アプリID)
3-3. ゲートPIN
3-4. ユーザPIN要求
3-5. ユーザPIN入力
3-6. ユーザPIN
3-7. ユーザPIN検証
3-8. PINを送信
3-9. PIN検証
3-10. 処理

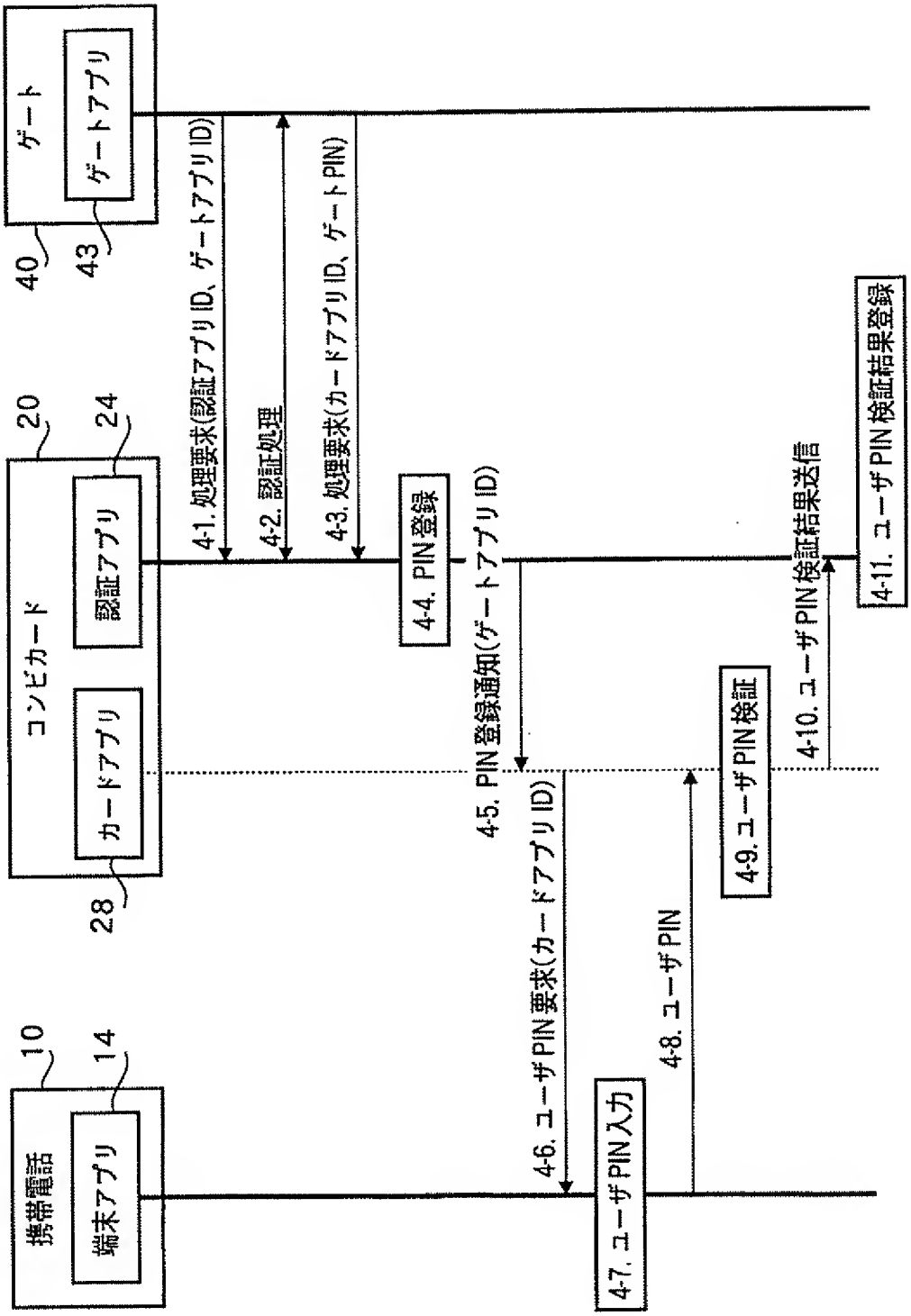
[図16]


ゲート
ゲートアプリ
40
43
コンビカード
認証アプリ
カードアプリ
20
24
29
携帯電話
端末アプリ
10
14
4-1. 処理要求(認証アプリID、ゲートアプリID)
4-2. 認証処理
4-3. 処理要求(カードアプリID、ゲートPIN)
4-4. PIN登録
4-5. ユーザPIN要求(アプリ2ID)
4-6. ユーザPIN入力
4-7. ユーザPIN
4-8. ユーザPIN登録

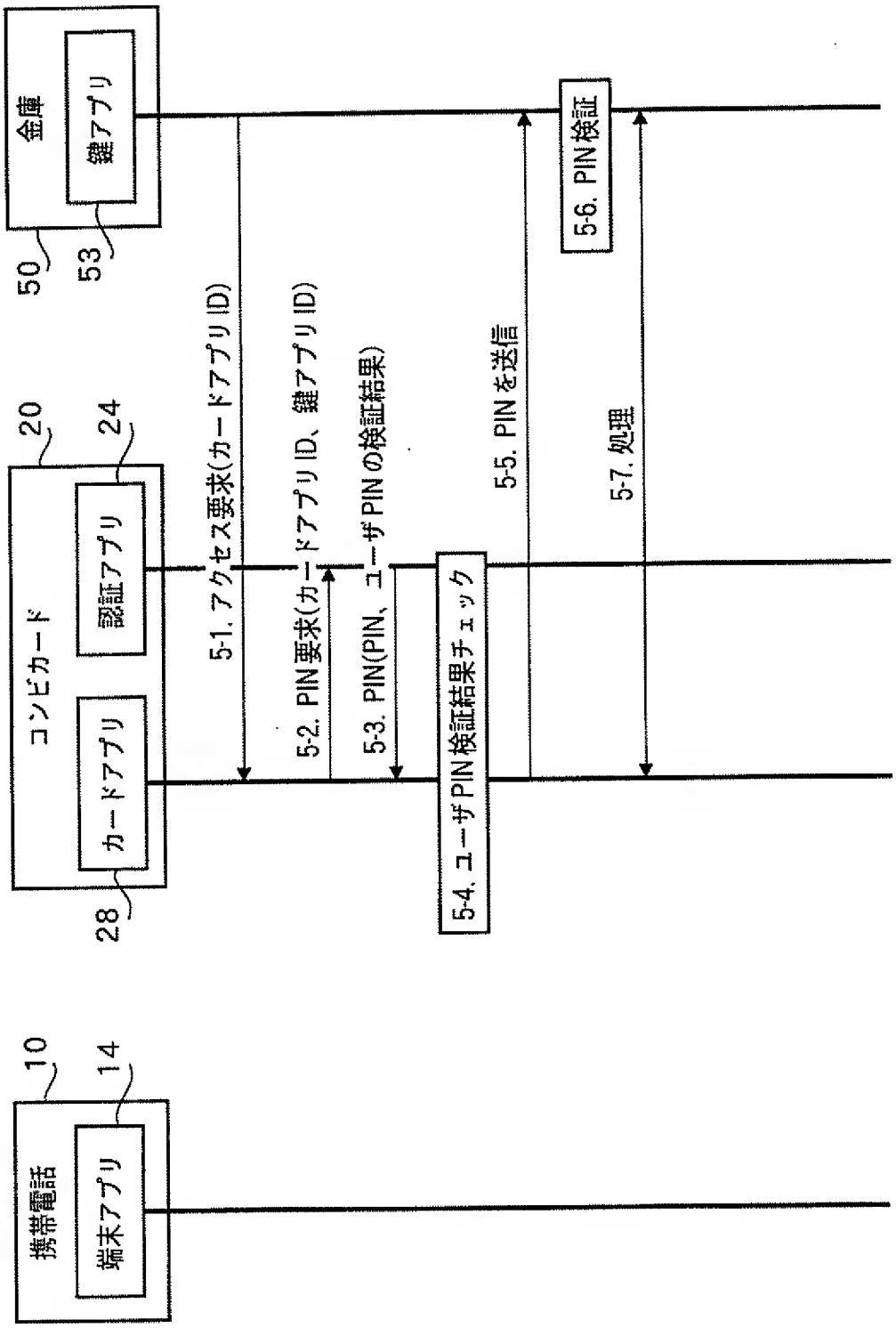
[図17]


金庫
鍵アプリ
50
53
コンビカード
認証アプリ
カードアプリ
20
24
28
携帯電話
端末アプリ
15
14
5-1. アクセス要求(カードアプリID)
5-2. PIN要求(カードアプリID、鍵アプリID)
5-3. PIN(PIN、ユーザPIN)
5-4. ユーザPIN検証
5-5. PINを送信
5-6. PIN検証
5-7. 処理

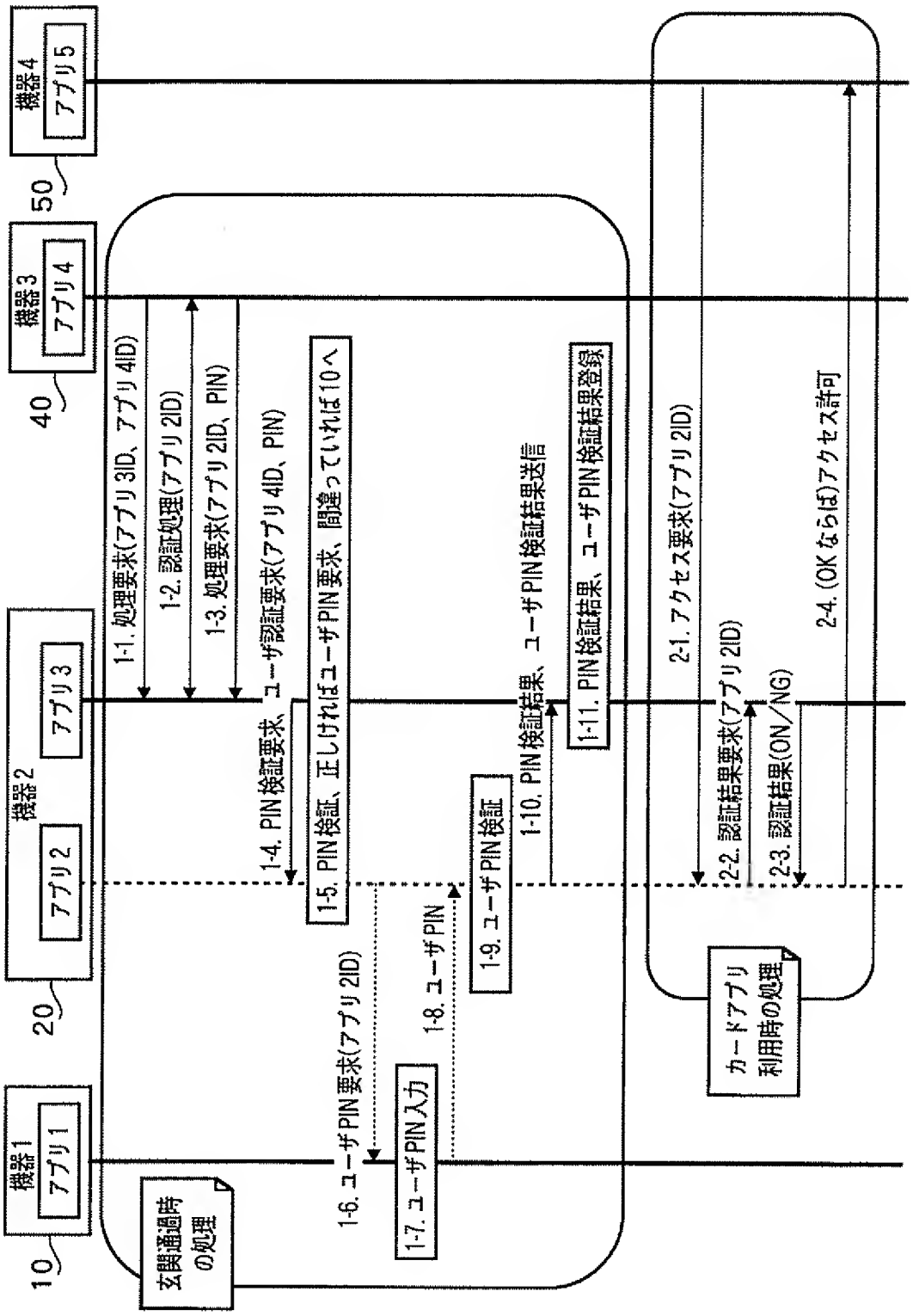
[図18]


ゲート
ゲートアプリ
40
43
コンビカード
認証アプリ
カードアプリ
20
24
28
携帯電話
端末アプリ
10
14
4-1. 処理要求(認証アプリID、ゲートアプリID)
4-2. 認証処理
4-3. 処理要求(カードアプリID、ゲートPIN)
4-4. PIN登録
4-5. PIN登録通知(ゲートアプリID)
4-6. ユーザPIN要求(カードアプリID)
4-7. ユーザPIN入力
4-8. ユーザPIN
4-9. ユーザPIN検証
4-10. ユーザPIN検証結果送信
4-11. ユーザPIN検証結果登録

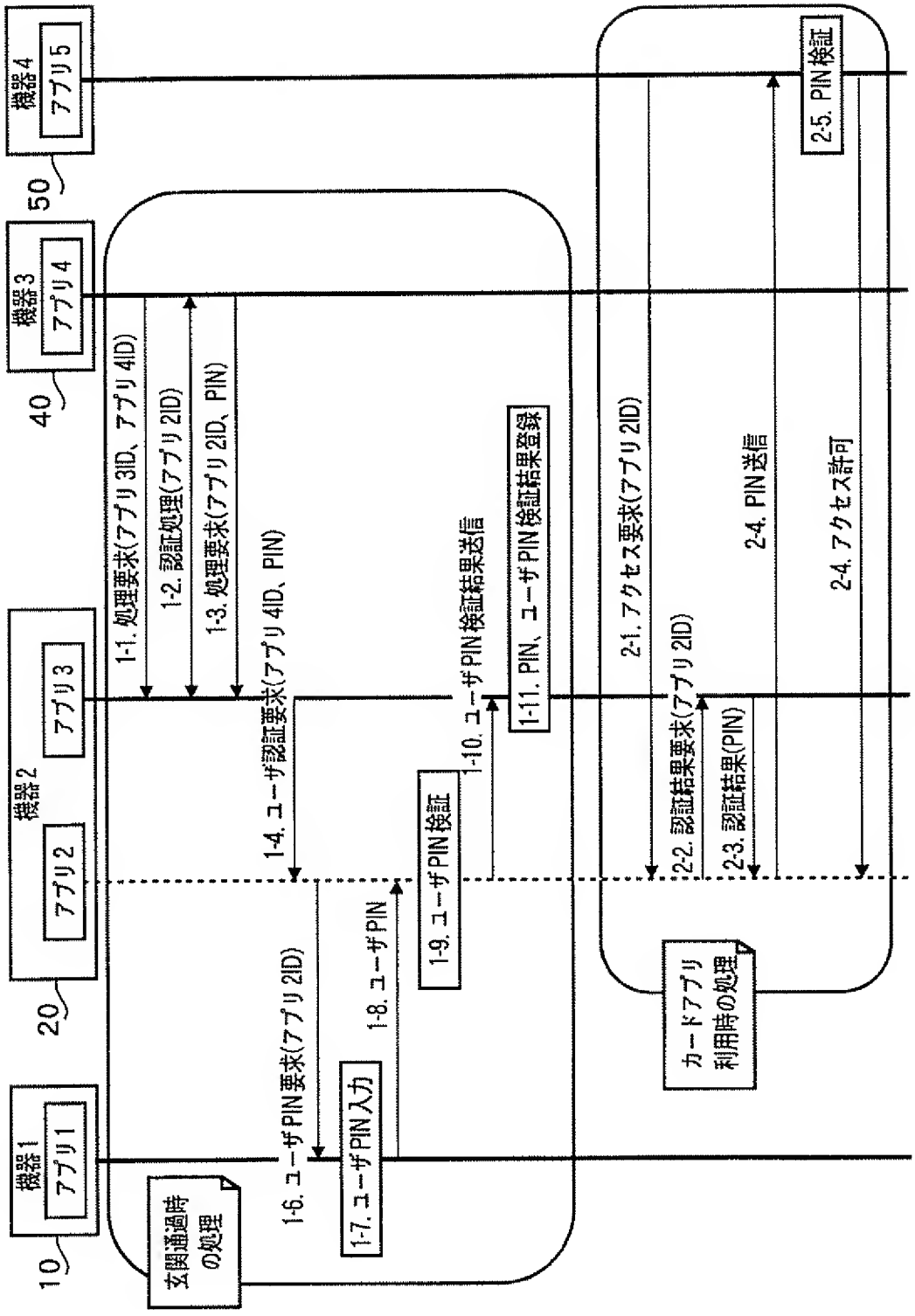
[図19]


金庫
鍵アプリ
50
53
コンビカード
認証アプリ
カードアプリ
20
24
28
携帯電話
端末アプリ
10
14
5-1. アクセス要求(カードアプリ ID)
5-2. PIN 要求(カードアプリ ID、鍵アプリ ID)
5-3. PIN(PIN、ユーザ PIN の検証結果)
5-4. ユーザ PIN 検証結果チェック
5-5. PIN を送信
5-6. PIN 検証
5-7. 処理

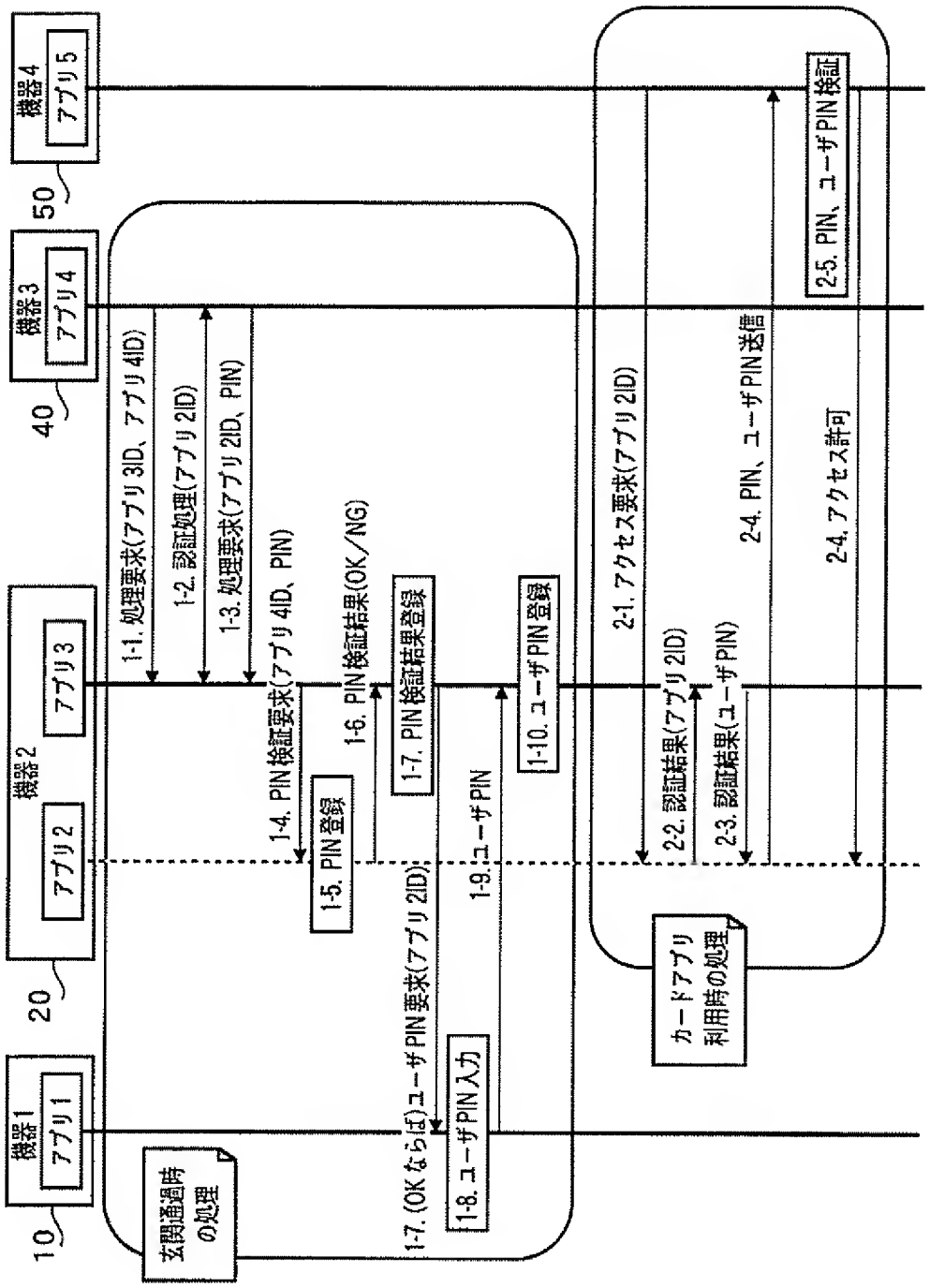
[図20]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
玄関通過時の処理
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. PIN検証要求、ユーザ認証要求(アプリ4ID、PIN)
1-5. PIN検証、正しければユーザPIN要求、間違っていれば10へ
1-6. ユーザPIN要求(アプリ2ID)
1-7. ユーザPIN入力
1-8. ユーザPIN
1-9. ユーザPIN検証
1-10. PIN検証結果、ユーザPIN検証結果送信
1-11. PIN検証結果、ユーザPIN検証結果登録
カードアプリ利用時の処理
2-1. アクセス要求(アプリ2ID)
2-2. 認証結果要求(アプリ2ID)
2-3. 認証結果(ON/NG)
2-4. (OKならば)アクセス許可

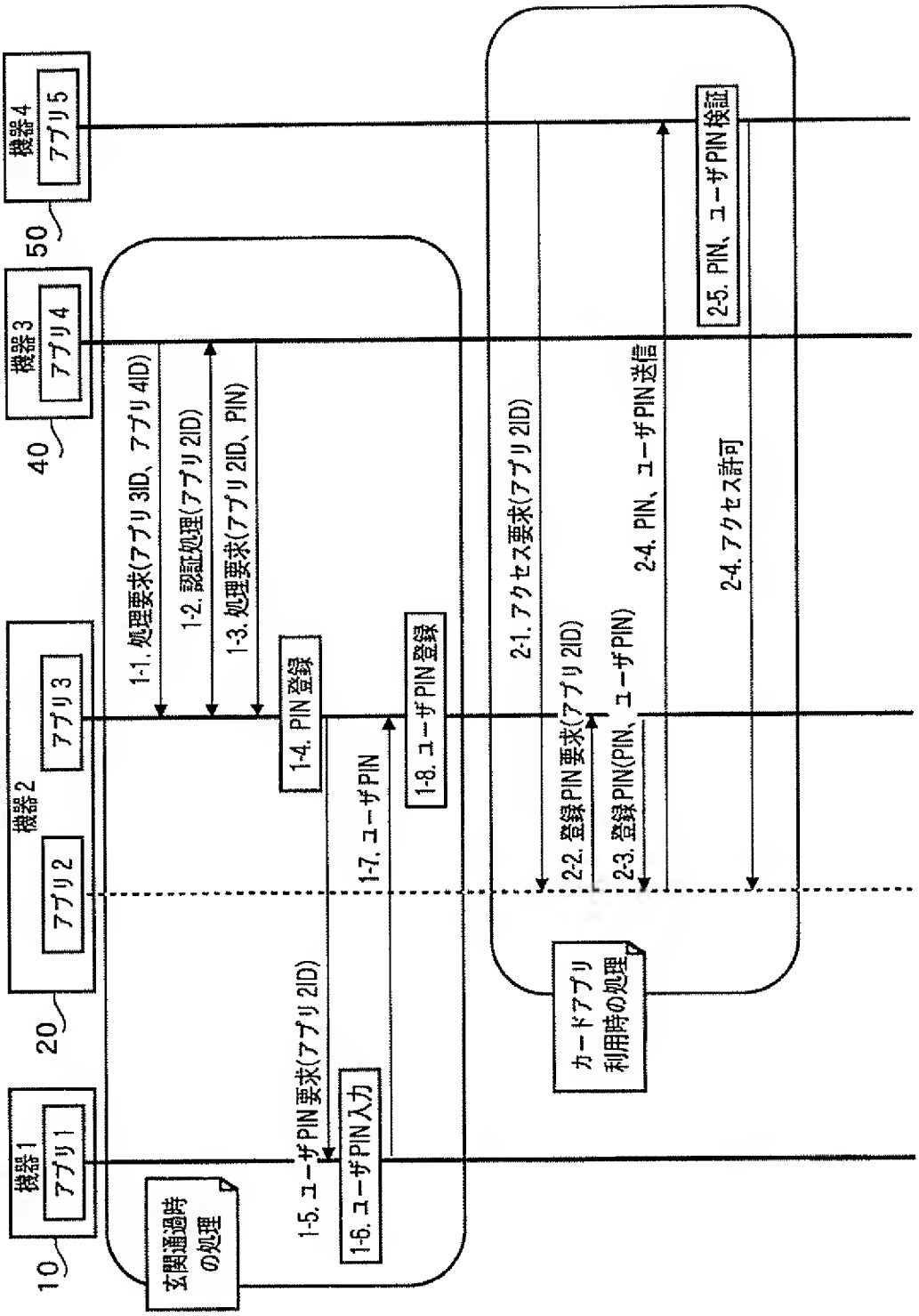
[図21]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. ユーザ認証要求(アプリ4ID、PIN)
1-6. ユーザPIN要求(アプリ2ID)
1-7. ユーザPIN入力
1-8. ユーザPIN
1-9. ユーザPIN検証
1-10. ユーザPIN検証結果送信
1-11. PIN、ユーザPIN検証結果登録
玄関通過時の処理
2-1. アクセス要求(アプリ2ID)
2-2. 認証結果要求(アプリ2ID)
2-3. 認証結果(PIN)
2-4. PIN送信
2-5. PIN検証
2-4. アクセス許可
カードアプリ利用時の処理

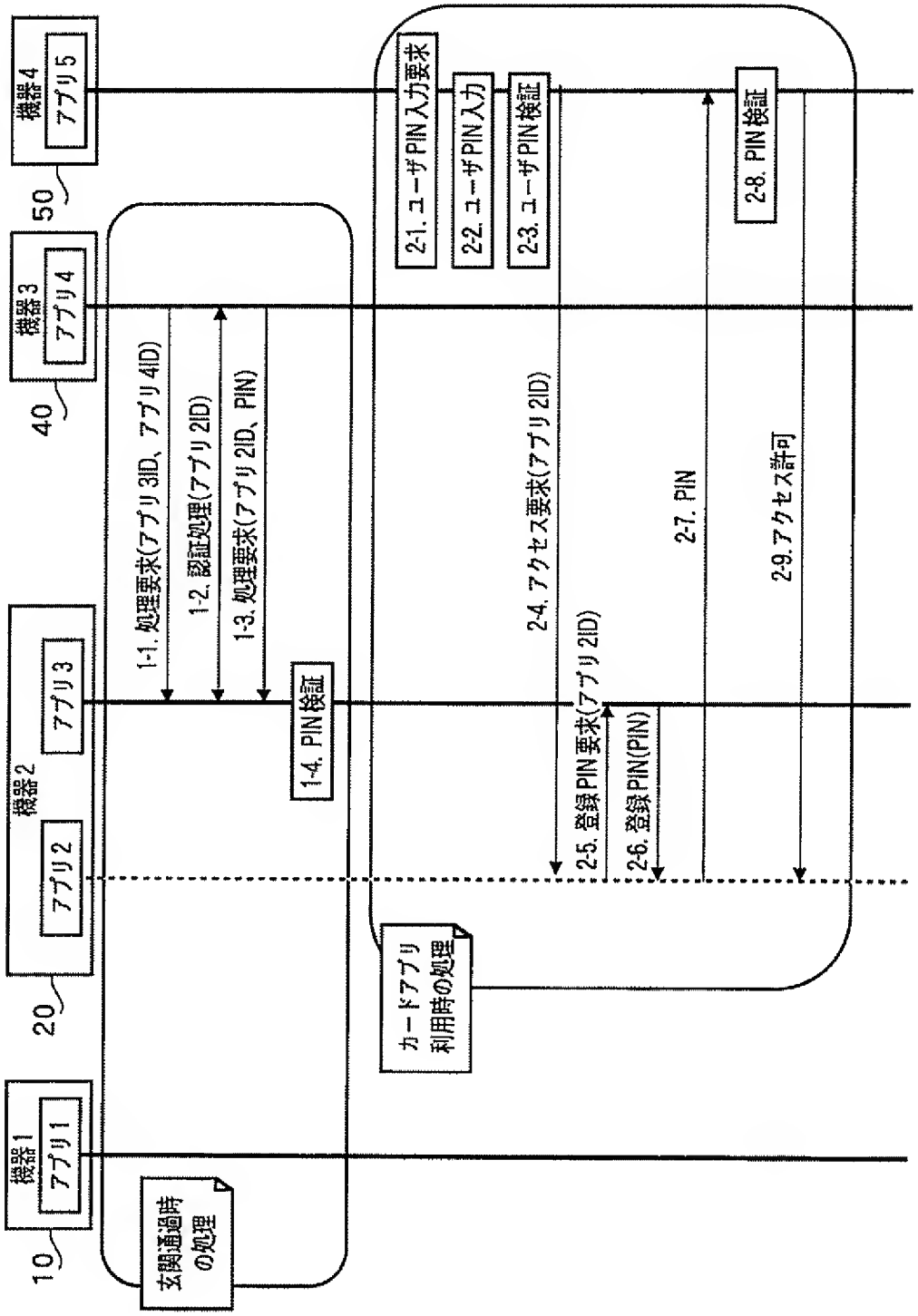
[図22]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
玄関通過時の処理
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. PIN検証要求(アプリ4ID、PIN)
1-5. PIN登録
1-6. PIN検証結果(OK/NG)
1-7. PIN検証結果登録
1-7. (OKならば)ユーザPIN要求(アプリ2ID);
1-8. ユーザPIN入力
1-9. ユーザPIN
1-10. ユーザPIN登録
カードアプリ利用時の処理
2-1. アクセス要求(アプリ2ID)
2-2. 認証結果(アプリ2ID)
2-3. 認証結果(ユーザPIN)
2-4. PIN、ユーザPIN送信
2-4. アクセス許可
2-5. PIN、ユーザPIN検証

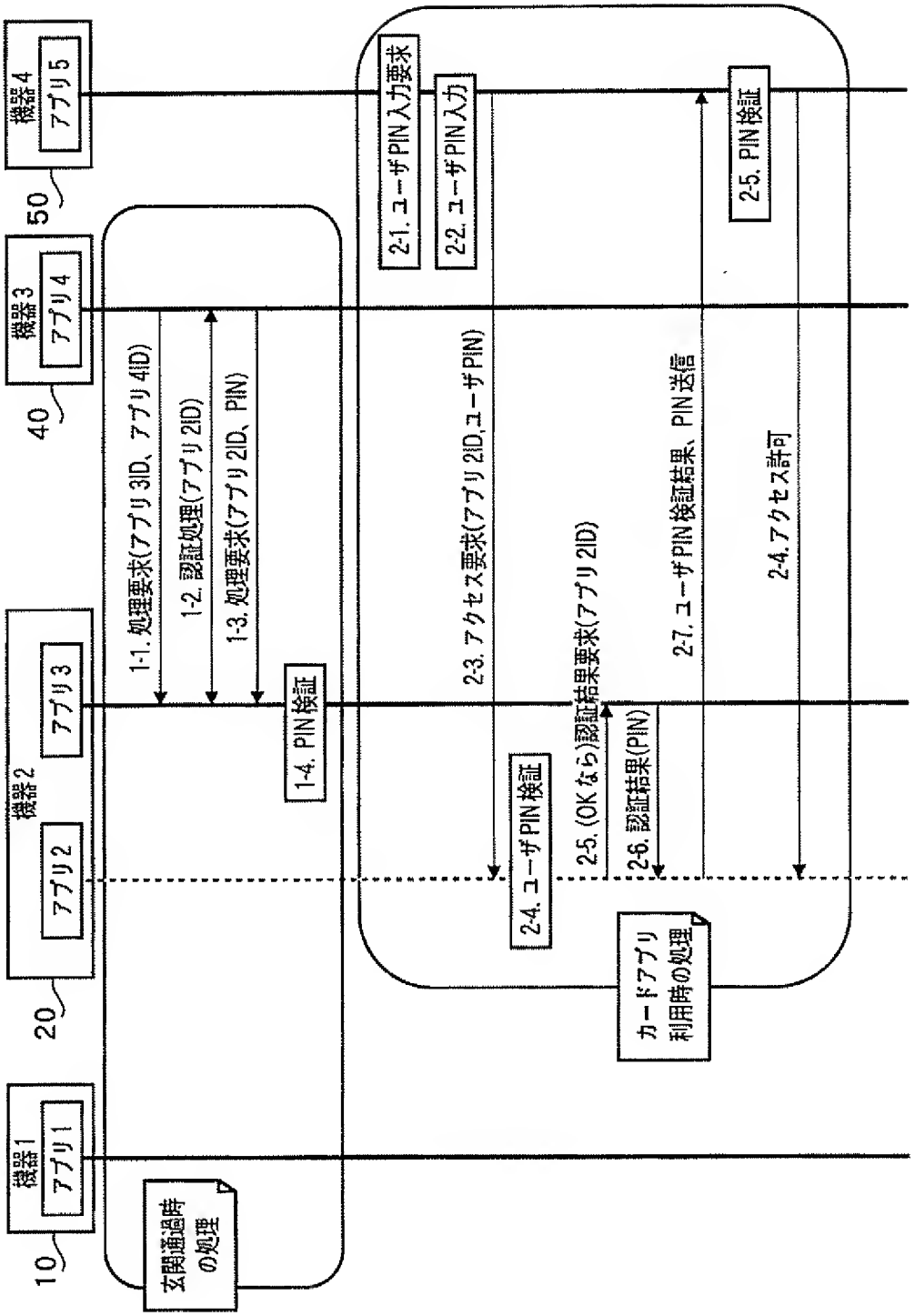
[図23]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
玄関通過時の処理
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. PIN登録
1-5. ユーザPIN要求(アプリ2ID)
1-6. ユーザPIN入力
1-7. ユーザPIN
1-8. ユーザPIN登録
カードアプリ利用時の処理
2-1. アクセス要求(アプリ2ID)
2-2. 登録PIN要求(アプリ2ID)
2-3. 登録PIN(PIN、ユーザPIN)
2-4. PIN、ユーザPIN送信
2-4. アクセス許可
2-5. PIN、ユーザPIN検証

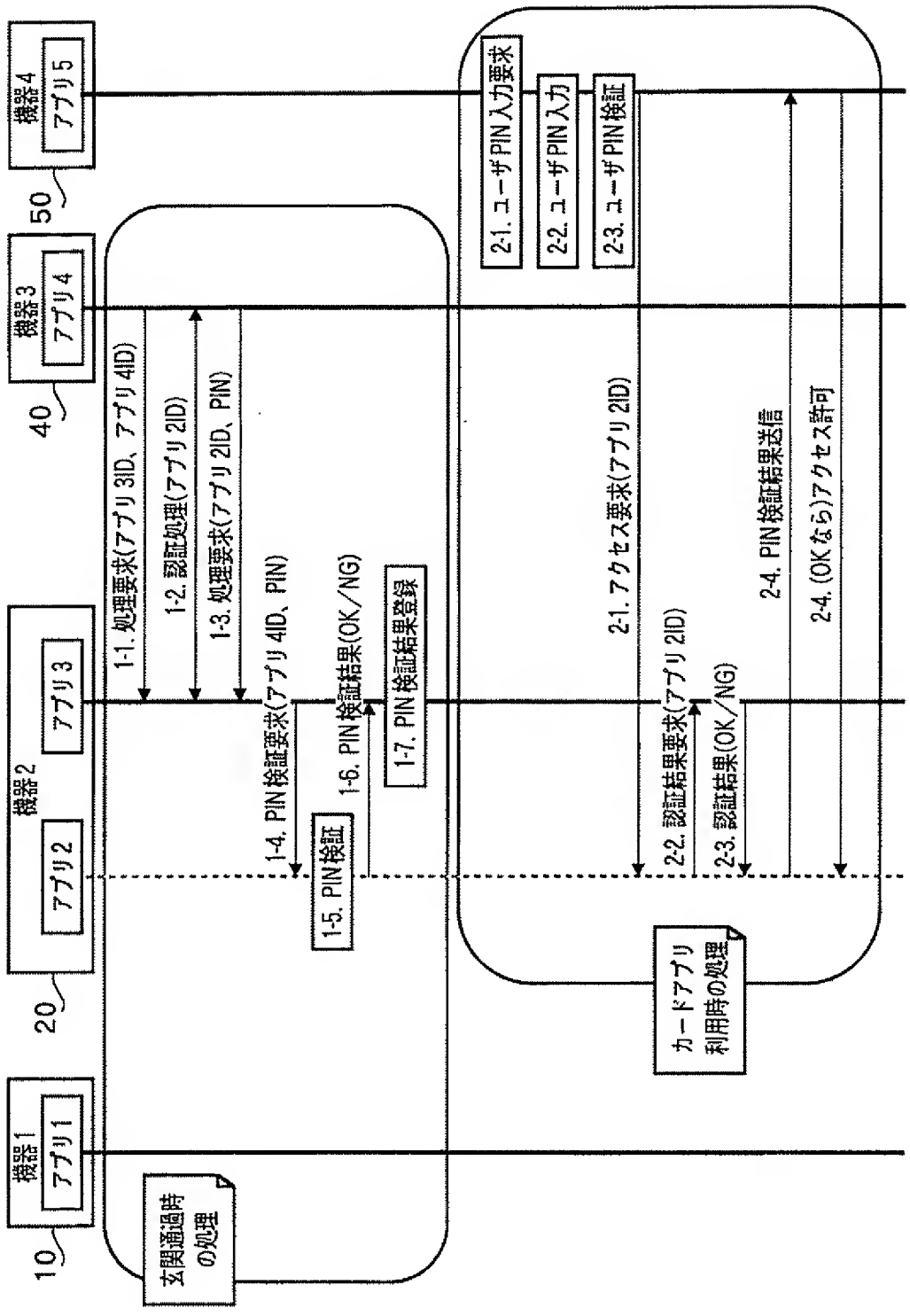
[図24]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
玄関通過時の処理
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. PIN検証
カードアプリ利用時の処理
2-1. ユーザPIN入力要求
2-2. ユーザPIN入力
2-3. ユーザPIN検証
2-4. アクセス要求(アプリ2ID)
2-5. 登録PIN要求(アプリ2ID)
2-6. 登録PIN(PIN)
2-7. PIN
2-8. PIN検証
2-9. アクセス許可

[図25]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
玄関通過時の処理
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. PIN検証
カードアプリ利用時の処理
2-1. ユーザPIN入力要求
2-2. ユーザPIN入力
2-3. アクセス要求(アプリ2ID,ユーザPIN)
2-4. ユーザPIN検証
2-5. (OKなら)認証結果要求(アプリ2ID)
2-6. 認証結果(PIN)
2-7. ユーザPIN検証結果、PIN送信
2-4. アクセス許可
2-5. PIN検証

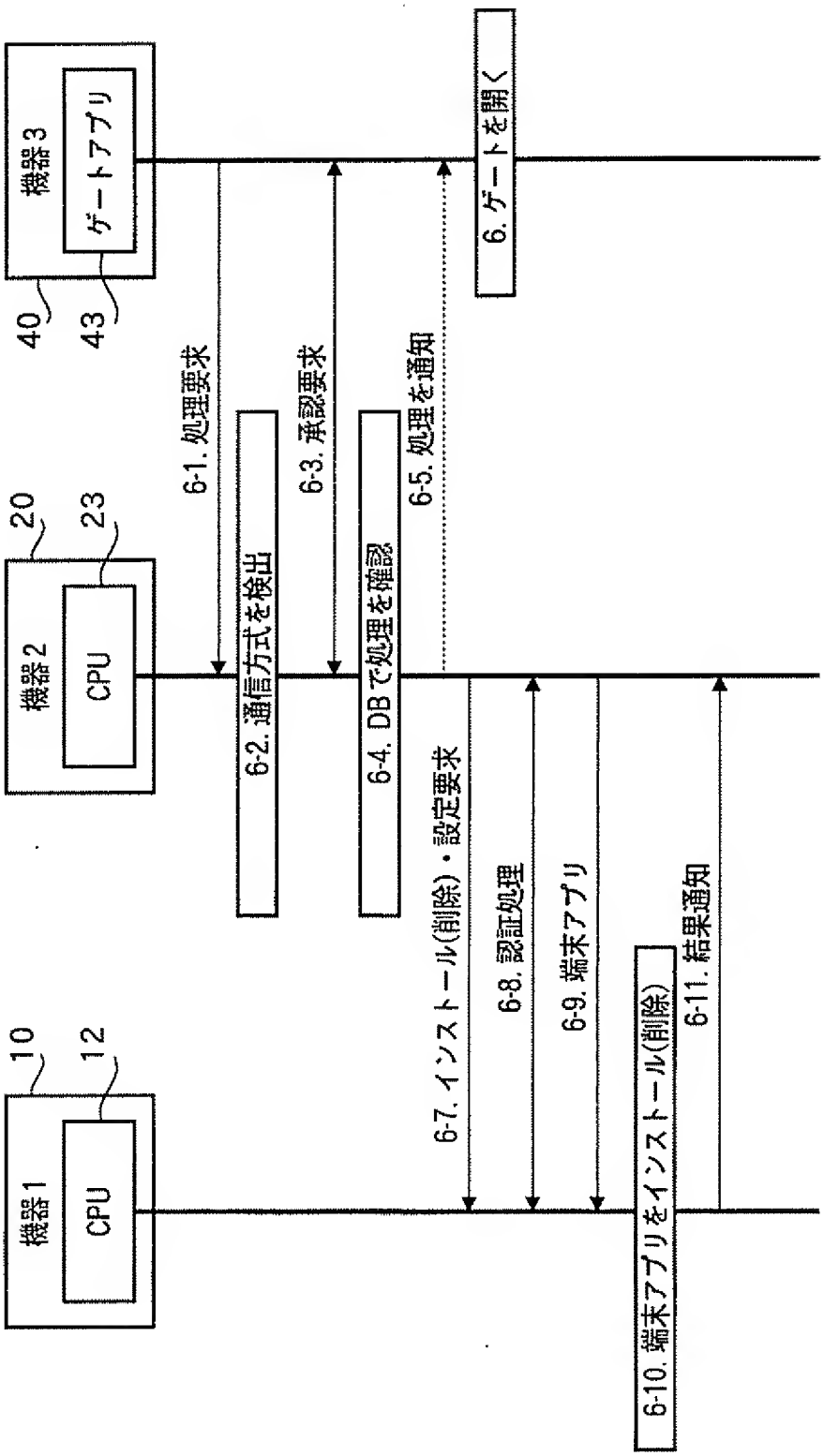
[図26]


機器1
アプリ1
10
機器2
アプリ2
アプリ3
20
機器3
アプリ4
40
機器4
アプリ5
50
玄関通過時の処理
1-1. 処理要求(アプリ3ID、アプリ4ID)
1-2. 認証処理(アプリ2ID)
1-3. 処理要求(アプリ2ID、PIN)
1-4. PIN検証要求(アプリ4ID、PIN)
1-5. PIN検証
1-6. PIN検証結果(OK/NG)
1-7. PIN検証結果登録
2-1. ユーザPIN入力要求
2-2. ユーザPIN入力
2-3. ユーザPIN検証
2-1. アクセス要求(アプリ2ID)
2-2. 認証結果要求(アプリ2ID)
2-3. 認証結果(OK/NG)
2-4. PIN検証結果送信
2-4. (OKなら)アクセス許可
カードアプリ利用時の処理

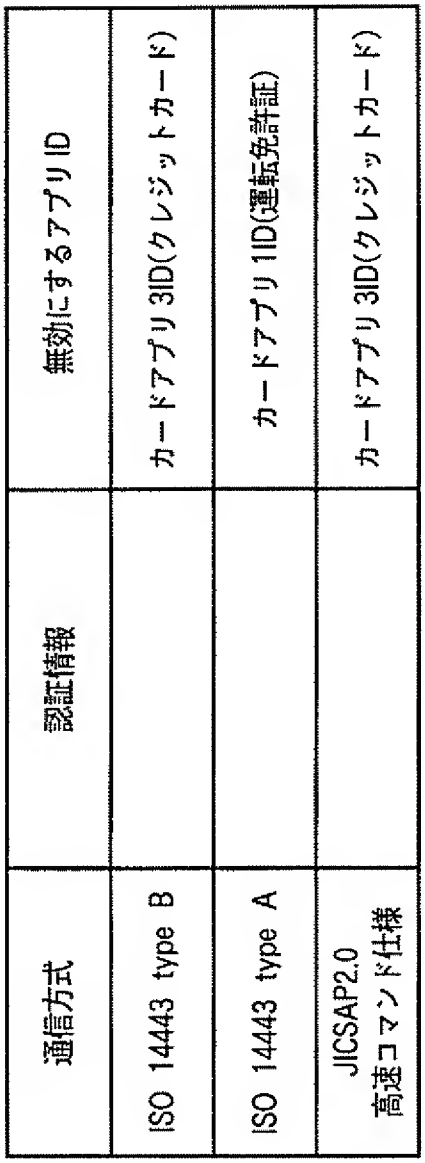
[図27]

ID	ゲートアプリID	通信方式	認証情報	インストール可能な端末アプリ設定命令ID	削除する端末アプリ設定命令ID
1	www.app.co.jp/gate1	独自通信方式A		端末アプリID(個人用メーラ) 端末アプリ2ID(ゲーム) 設定命令5ID(個人のネットワーク設定、壁紙、通常通話モード)	端末アプリ3ID(内線番号閲覧ブラウザ) 設定命令7ID(会社用設定：会社のネットワーク設定、壁紙、内線モード)
2	www.app.co.jp/gate1	独自通信方式B		端末アプリID(会社用メーラ) 端末アプリ3ID(内線番号閲覧ブラウザ) 設定命令7ID(会社用設定：会社のネットワーク設定、壁紙、内線モード)	端末アプリID(個人用メーラ) 端末アプリ2ID(ゲーム) 設定命令5ID(個人のネットワーク設定、壁紙、通常通話モード)

[図28]

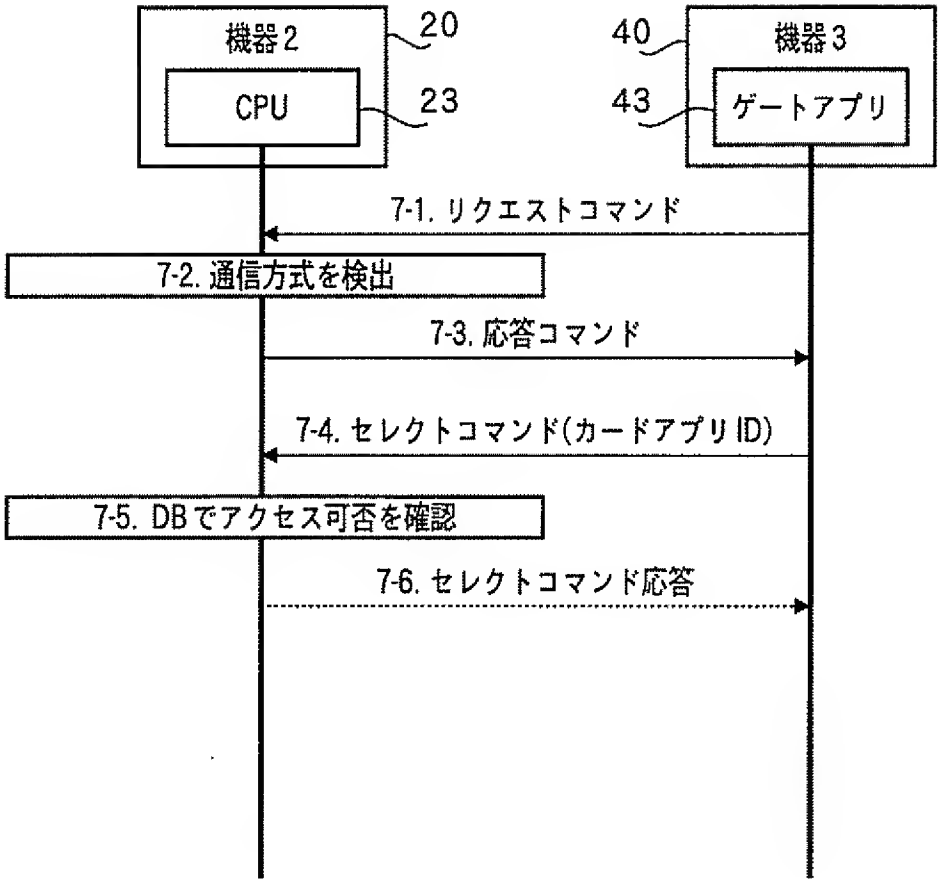

機器3
ゲートアプリ
40
43
6. ゲートを開く
6-1. 処理要求
6-3. 承認要求
6-5. 処理を通知
20
23
機器2
CPU
6-2. 通信方式を検出
6-4. DBで処理を確認
6-7. インストール(削除)・設定要求
6-8. 認証処理
6-9. 端末アプリ
6-11. 結果通知
10
12
機器1
CPU
6-10. 端末アプリをインストール(削除)

[図29]

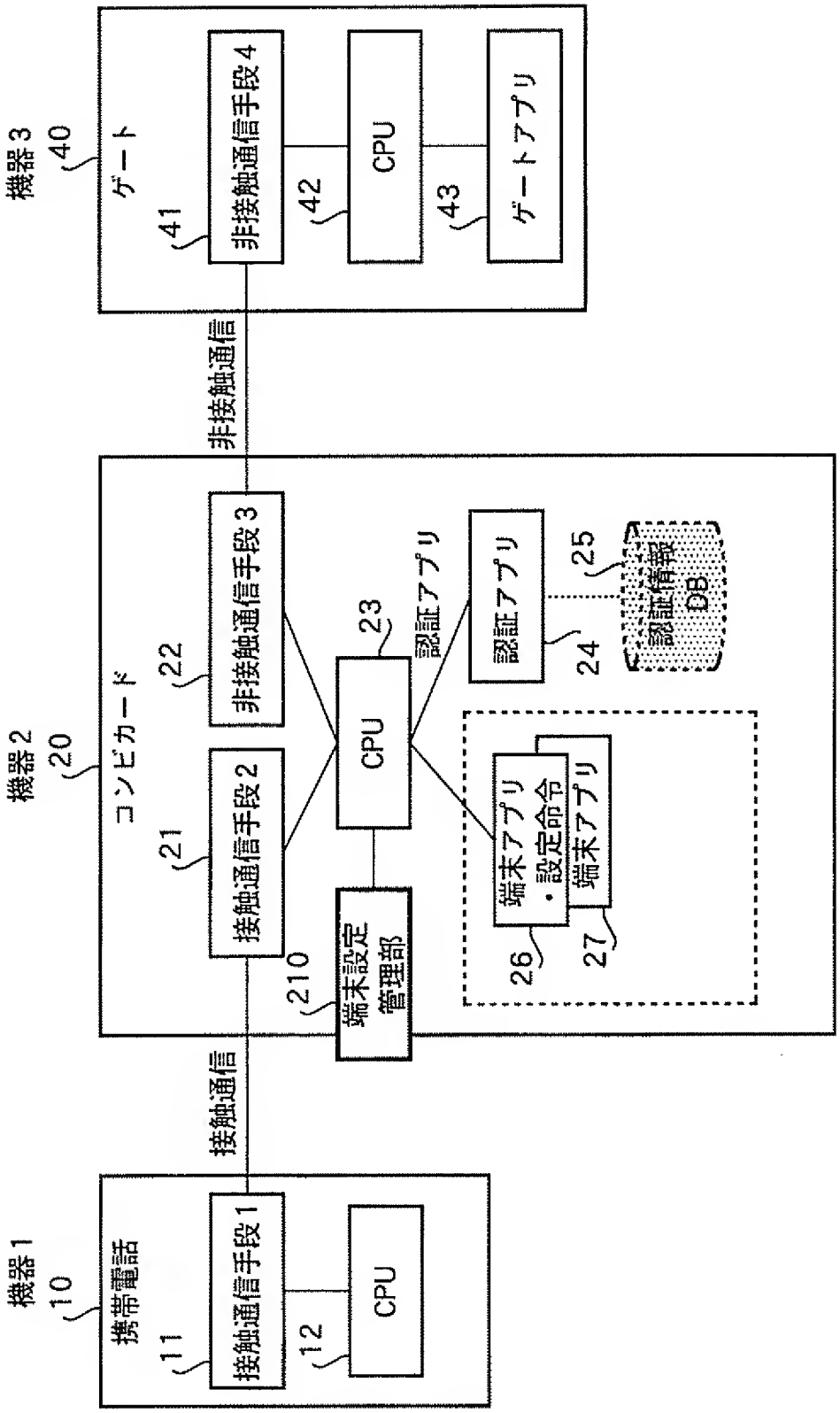


通信方式	認証情報	無効にするアプリID
ISO 14443 type B		カードアプリ3ID(クレジットカード)
ISO 14443 type A		カードアプリ1ID(運転免許証)
JICSAP2.0 高速コマンド仕様		カードアプリ3ID(クレジットカード)

[図30]


機器2
20
CPU
23
40
機器3
43
ゲートアプリ
7-1. リクエストコマンド
7-2. 通信方式を検出
7-3. 応答コマンド
7-4. セレクトコマンド(カードアプリID)
7-5. DBでアクセス可否を確認
7-6. セレクトコマンド応答

[図31]


機器1
10
携帯電話
11
接触通信手段1
12
CPU
接触通信
機器2
20
コンビカード
21
接触通信手段2
22
非接触通信手段3
210
端末設定管理部
23
CPU
認証アプリ
24
認証アプリ
25
認証情報DB
26
端末アプリ・設定命令
27
端末アプリ
非接触通信
機器3
40
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ

[図32]

ID	ゲートアプリID	通信方式	認証情報	有効除間	インストール可能な端末アプリ 設定命令ID	削除する端末アプリ 設定命令ID
1	www.app.co.jp/gate1	ISO14 443typeB		5：00	端末アプリ3ID(内線番号閲覧ブラウザ) 設定命令7ID(会社用設定：会社のネットワーク設定、壁紙、内蔵モード)	端末アプリ2ID(ゲーム) 設定命令5ID(個人のネットワーク設定、壁紙、通信通話モード)
2	www.app.co.jp/gate2	UWB		制限なし	端末アプリ2ID(ゲーム) 設定命令5ID(個人のネットワーク設定、壁紙、通信通話モード)	端末アプリ3ID(内線番号閲覧ブラウザ) 設定命令7ID(会社用設定：会社のネットワーク設定、壁紙、内蔵モード)

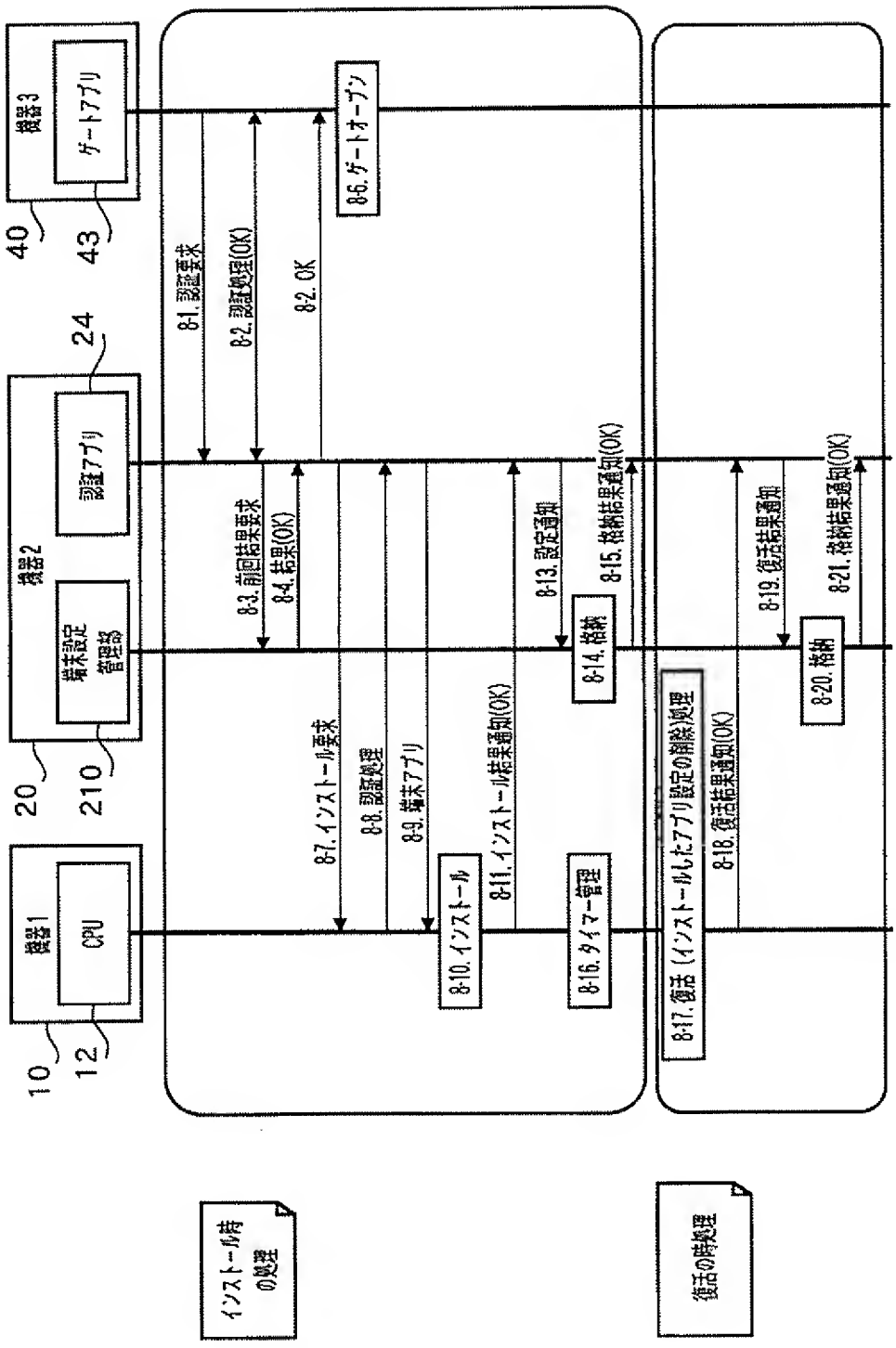
[図33]

図34の8－14で格納されるデータの例

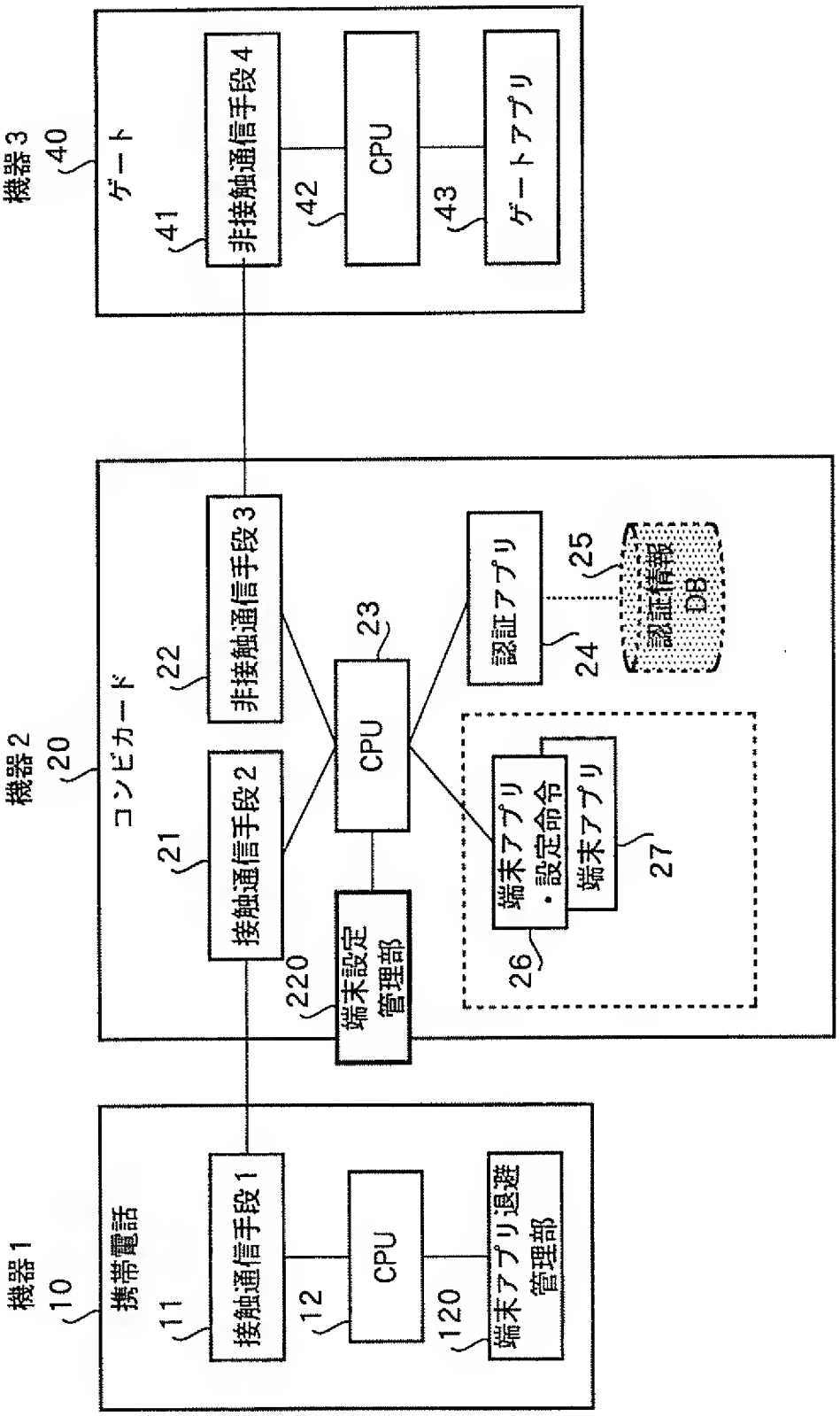
図34の8－20で格納されるデータの例

ID	機器3ID	ゲートアプリID	機器1ID	設定時のタイムスタンプ	有効時間	認証設定DBのID	インストールした端末アプリID	インストールした設定命令ID	削除した端末アプリID	削除した設定アプリID	設定処理結果	復活通知時のタイムスタンプ	復活処理結果
1	www.app.co.jp/gateterminal1	www.app.co.jp/gateapp1	www.app.co.jp/terminal1	2004/12/24 15:32:02	5:00	1	端末アプリ3ID (内線番号閲覧ブラウザ)	設定命令7ID (会社用設定:会社のネットワーク設定、壁紙、内線モード)	端末アプリ2ID (ゲーム)	設定命令5ID (個人のネットワーク設定 壁紙、通常通話モード)	正常	2004/12/24 23:32:02	正常

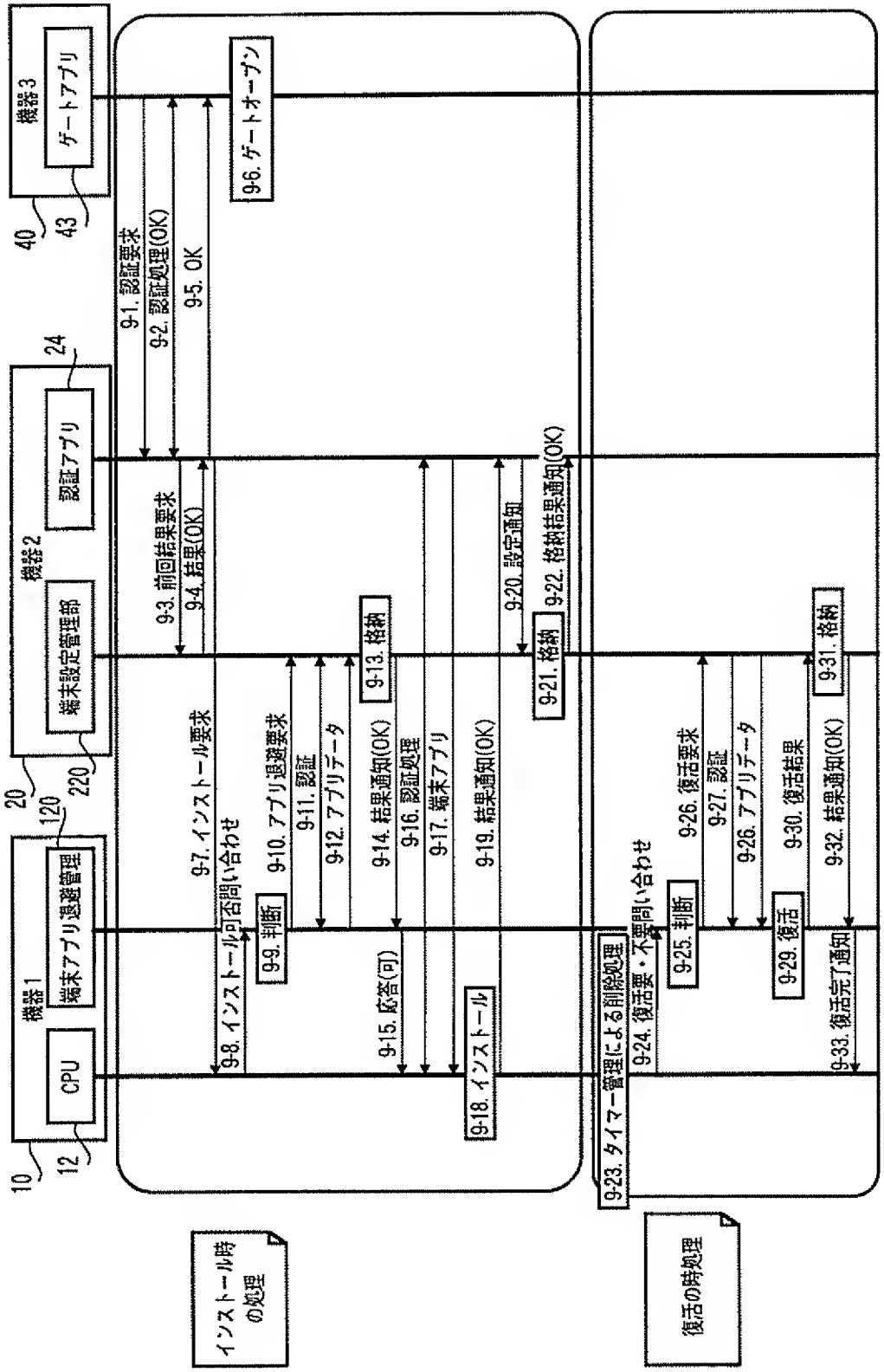
[図34]


機器1
CPU
10
12
機器2
端末設定管理部
認証アプリ
20
210
24
機器3
ゲートアプリ
40
43
8-1.認証要求
8-2.認証処理(OK)
8-2. OK
8-3.前回結果要求
8-4.結果(OK)
8-6.ゲートオープン
8-7.インストール要求
8-8.認証処理
8-9.端末アプリ
8-10.インストール
8-11.インストール結果通知(OK)
8-13.設定通知
8-14.格納
8-15.格納結果通知(OK)
8-16.タイマー管理
8-17.復活(インストールしたアプリ設定の削除)処理
8-18.復活結果通知(OK)
8-19.復活結果通知
8-20.格納
8-21.格納結果通知(OK)
インストール時の処理
復活の時処理

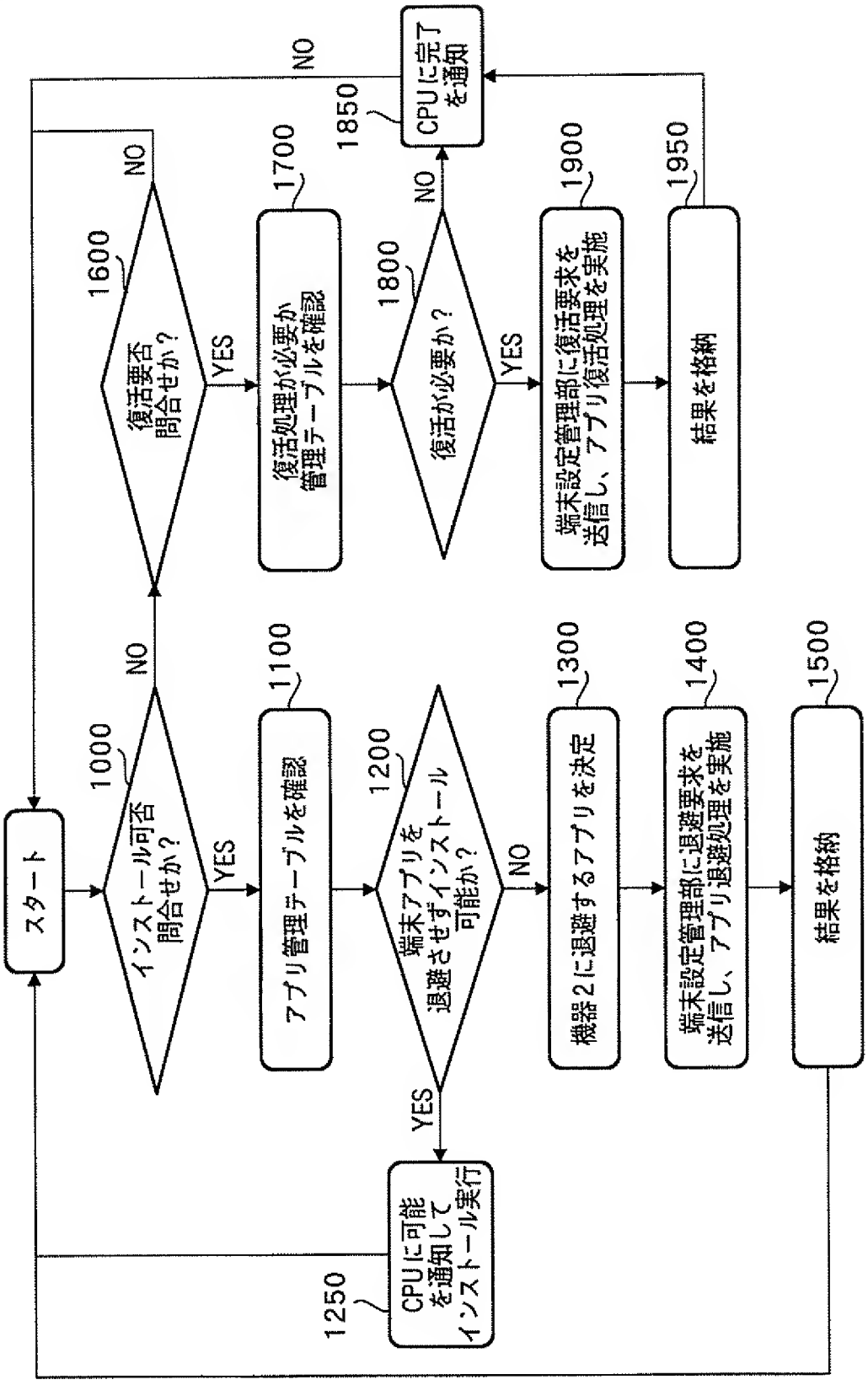
[図35]


機器1
10
携帯電話
11
接触通信手段1
12
CPU
120
端末アプリ退避管理部
機器2
20
コンビカード
21
接触通信手段2
22
非接触通信手段3
23
CPU
220
端末設定管理部
24
認証アプリ
25
認証情報DB
26
端末アプリ・設定命令
27
端末アプリ
機器3
40
ゲート
41
非接触通信手段4
42
CPU
43
ゲートアプリ

[図36]


機器1
CPU
端末アプリ退避管理
機器2
端末設定管理部
認証アプリ
機器3
ゲートアプリ
9-1. 認証要求
9-2. 認証処理(OK)
9-3. 前回結果要求
9-4. 結果(OK)
9-5. OK
9-6. ゲートオープン
9-7. インストール要求
9-8. インストール可否問い合わせ
9-9. 判断
9-10. アプリ退避要求
9-11. 認証
9-12. アプリデータ
9-13. 格納
9-14. 結果通知(OK)
9-15. 応答(可)
9-16. 認証処理
9-17. 端末アプリ
9-18. インストール
9-19. 結果通知(OK)
9-20. 設定通知
9-21. 格納
9-22. 格納結果通知(OK)
9-23. タイマー管理による削除処理
9-24. 復活要・不要問い合わせ
9-25. 判断
9-26. 復活要求
9-27. 認証
9-28. アプリデータ
9-29. 復活
9-30. 復活結果
9-31. 格納
9-32. 結果通知(OK)
9-33. 復活完了通知
インストール時の処理
復活の時処理

[図37]


スタート
インストール可否問合せか？
1000
NO
YES
アプリ管理テーブルを確認
1100
端末アプリを退避させずインストール可能か？
1200
YES
NO
CPUに可能を通知してインストール実行
1250
機器2に退避するアプリを決定
1300
端末設定管理部に退避要求を送信し、アプリ退避処理を実施
1400
結果を格納
1500
復活要否問合せか？
1600
NO
YES
復活処理が必要か管理テーブルを確認
1700
復活が必要か？
1800
NO
YES
CPUに完了を通知
1850
端末設定管理部に復活要求を送信し、アプリ復活処理を実施
1900
結果を格納
1950
NO